



City Research Online

City St George's, University of London

Citation: Lucic, I. (2010). Risk and Safety in Engineering Processes.
(Unpublished Doctoral thesis, City University London)

This is the submitted version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: <https://city-ref-test.eprints-hosting.org/id/eprint/8719/>

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to [City Research Online policy](#).



CITY UNIVERSITY
LONDON

Risk and Safety in Engineering Processes

by
IVAN LUCIC

**A THESIS SUBMITTED FOR THE AWARD OF THE
DEGREE OF DOCTOR OF PHILOSOPHY
IN SYSTEMS AND MODELLING**

SYSTEMS AND CONTROL RESEARCH CENTRE
SCHOOL OF ENGINEERING AND MATHEMATICAL SCIENCES

CITY UNIVERSITY
LONDON EC1V 0HB
September 2010

Acknowledgments

My life and my research would be impossible without the love and support from my loving wife Marija and the joy and inspiration brought to me by our daughter Anka and son Lazar. I will always be grateful to my wife for her loyal support whenever and whatever I did, however foolish it may have been.

I am extremely grateful to Prof Nicos Karcianas and Prof Ali Hessami for their patience, guidance and above all friendship. It was them who tricked me into commencing this expedition into the enchanted world of research where everything is possible. I am grateful to Nicos for his support, advice and guidance. His constructive criticism and observations focussed my thoughts and directed my journey. I owe immense debt to Ali, for all the knowledge and understanding of systems and safety theory and practice, long discussions about ethics, help and support and trust he had in me all this years.

I am grateful for my mother's persistent, subtle encouragement to complete the research and my father's nonchalant faith in me.

I am immensely thankful to friends and colleagues from my team in LU who work with me, patiently enhancing my understanding and stubbornly helping me to implement my ideas on very challenging projects. So thank you, very much, Alison Danahay, Chi Wang, Josh Ahmed, Lucy Regan, Michael Mangroo, Mike Lester, Mukesh Sharma, Nelly Christophylaki, Paul Lawless, Peter Littlejohns, Peter Stanley, Roger Short, Ricardo Hetherington and Tim Ballantyne.

Abstract

This research project focused on the treatment of safety risks in railways. Existing methodologies for assessment and management of the safety risk on railways are mostly empirical and have been developed out of a need to satisfy the regulatory requirements and in response to a number of major accidents. Almost all of these processes and methodologies have been developed in support of approvals of specific products or very simple systems and do not add up to a holistic coherent methodology suited for analysis of modern, complex systems, involving many vastly different constituents (software, hardware, people, products developed in different parts of the world, etc.). The complexities of modern railway projects necessitate a new approach to risk analysis and management.

At the outset, the focus of the research was on the organisation of the family of existing system analysis methodologies into a coherent, heterogeneous methodology. An extensive review of existing methodologies and processes was undertaken and is summarised in this thesis. Relationships between different methodologies and their properties were investigated seeking to define the rules for embedding these into a hierarchical nest and relating their emergent properties.

Four projects were utilised as case studies for the evaluation of existing methodologies and processes and initial development.

This thesis describes the methodology adopted in support of development of the System Safety Case and the structure of the document.

Based on that experience and knowledge a set of high level requirements was identified for an integrated, holistic system safety analysis and management process. A framework consisting of existing and novel methodologies and processes was developed and trialled on a real life project. During the trial several gaps in the process were identified and adequate new methodologies or processes defined and implemented to complete the framework.

The trial was very successful and the new framework, referred to as the Engineering Safety Case Management Process is implemented across the London Underground Upgrades Directory.

Key words: Risk modelling, Systems Approach, Holistic, Safety Case, Systems Assurance, Change Safety Analysis, System Safety, System Integration.

The whole is more than the sum of its parts. The part is more than a fraction of the whole – Aristotle

Contents:

CHAPTER 1: Introduction	11
1.1 Problem area	11
1.2 Objectives and Aim of the Research	12
1.3 Structure of this thesis	13
1.4 Definitions	15
1.5 Acronyms and Abbreviations	16
CHAPTER 2: Problem Definition	20
2.1 Chapter Introduction	20
2.2 History and Background (Waldrop, 1992), (Bernstein, 1996)	20
2.3 The Problem Area – detailed analysis	25
2.4 Chapter Conclusion	34
CHAPTER 3: Basic Systems Concept, Modelling Methodology and Background Literature	35
3.1 Chapter Introduction	35
Background to the notion of the system	35
3.3 The abstract notion of the system	39
3.4 Systems Thinking and Reasoning	42
3.5 Models and modelling	47
3.6 Review of existing analysis methodologies	49
3.6.1 System Description Models	49
3.6.2 System Dynamics	52
3.6.3 Risk Matrix (Rapid Ranking)	53
3.6.4 Failure Mode and Effects (and Criticality) Analysis	53
3.6.5 Theories of probability	54
3.6.6 Monte Carlo Simulation models	55
3.6.7 Theory of Evidence	56
3.6.8 Reliability Block Diagrams and Network models	57
3.6.9 Fault Trees - Event Trees	57
3.6.10 Markov models	59
3.6.11 Petri Nets	59
3.6.12 Theory of Fuzzy Sets	60
3.6.13 Weighted Factors Analysis	62
3.6.14 Advanced Cause – Consequence models	64

3.7 Chapter Conclusions	67
CHAPTER 4: The Application Area & Initial Development	69
4.1 Chapter introduction	69
4.2 First Project: Large Scale Safety Risk Modelling – ERTMS	71
4.2.1 Purpose and Scope of the Project.....	71
4.2.2 Problem Description and Conceptualisation.....	71
4.2.3 System representation and scoping	73
4.2.4 Focus and Identification.....	74
4.2.5 Core Hazards Modelling	76
4.2.6 Model Data.....	78
4.2.7 Integration of Individual Models into a Holistic System Safety Performance Model – Development.....	79
4.2.8 Output Generation and Normalisation	84
4.2.9 Risk Profiling	84
4.2.10 Derivation of Requirements	85
4.2.11 Optioneering application.....	87
4.3 Second Project: Axle Counter modelling.....	88
4.3.1 Purpose and Scope of the Project.....	88
4.3.2 Axle Counter Train Detection Concept.....	88
4.3.3 The Modelling Technique and the Tool.....	89
4.3.4 Analysis Approach.....	92
4.3.5 Tests	99
4.3.6 Application.....	101
4.4 Third Project: Complex Railway Project Safety Management – Manchester South Capacity Improvement Project	103
4.4.1 Purpose and Scope of the Project.....	103
4.4.2 Concept of Change Management	104
4.4.3 System Scoping and Conceptualisation	109
4.4.4 Identification and Analysis of Hazards	110
4.4.5 Comparative Risk Assessment.....	113
4.4.6 Management Process.....	115
4.5 Fourth Project: High Level Railway System Study - POLAND	118
4.5.1 Purpose and Scope of the Project.....	118
4.5.2 The Process for derivation of Safety & RAM requirements & Hazard Identification	120
4.5.3 System Scoping and Conceptualisation	122

4.5.4 Derivation of High Level Safety Requirements.....	125
4.5.5 Identification of Hazards.....	126
4.6 Chapter Conclusions	127
CHAPTER 5: Critique of current thinking, available tools and practice – a research agenda	129
5.1 Chapter Introduction	129
Figure 5-1: Structure of chapter 5	129
5.2 Summary of Requirements for new framework.....	129
5.3 Critique of current thinking.....	133
5.4 Chapter Conclusions	136
CHAPTER 6: A new systems based approach to system safety risk analysis and management	138
6.1 Chapter introduction	138
6.2 The Hazard	140
6.3 The Safety Case.....	146
6.4 Holistic Change Safety Analysis, Risk Assessment and Management Process.....	153
6.4.1 Engineering Safety and Assurance Process – Big Picture	153
6.4.2 The Change Safety Analysis and Risk Assessment and Management Process	157
6.4.3 Conceptualisation and Core Hazards Grouping	161
6.4.4 Initial Change Safety Analysis.....	164
6.4.5 Change Safety Analysis	165
6.4.6 Assertion of Completeness of System Analysis.....	174
6.4.7 Hazard Log, tool for Change Safety Management, Configuration Control and Reporting	176
6.4.8 Continual Appraisal and Knowledge Update.....	181
6.3 Chapter Conclusions	182
CHAPTER 7: Application	183
7.1 Chapter introduction	183
7.2 Background	185
7.3 Challenge	190
7.4 Identification of a set of common core hazards.....	196
7.5 Information gathering, conceptualisation and representation (System Analysis)...	199
7.6 Information processing	205
7.6.1 Change safety Analysis: hazard identification, analysis of causalities and consequences options and impact analysis and risk assessment.....	205

7.6.2 Restrictions management	209
7.6.3 Modelling	214
7.7 Derivation of safety requirements	232
7.8 Construction of the safety arguments logical network – Safety Justification & Case	234
7.8.1 Safety Justification	234
7.8.2 Safety Case	237
7.9 Assertion of completeness of analysis and assessment of uncertainties	249
7.9.1 Completeness of the safety arguments/facts net	250
7.10 Management and Reporting (Presentation of results)	251
7.10.1 Management	251
7.10.2 Reporting	253
7.11 Configuration Control, Continual Appraisal and Knowledge Management	254
7.11 Chapter Conclusions	259
CHAPTER 8: Conclusions, contribution and suggestions for future work	260
8.1 Conclusions and contribution	260
8.1.1 Overall summary	260
8.1.2 The concepts of “Hazard” and the “Safety case”	261
8.1.3 Holistic Change Safety Analysis, Risk Assessment and Management Process	261
8.1.4 Overall contribution	267
8.2 Future Work	267
CHAPTER 9: References and Bibliography	270
Papers and Reports published by author of the thesis	276
APPENDIX A: ALGORITHMS FOR APPORTIONMENT AND IMPORTANCE IN CAUSE-CONSEQUENCE MODELS	279
APPENDIX B: SPECIFICATION FOR CAUSE-CONSEQUENCE MODELS INTEGRATION ENVIRONMENT	285

List of figures:

Figure 1-1: Overall Structure of the thesis	14
Figure 2-1: Structure of Chapter 2	20
Figure 2-1: 7 Stage Process.....	28
Figure 3-1: Structure of chapter 3	35
Figure 3-2: Generalised presentation of the system.....	42
Figure 3-3: An example of the system decomposition model.....	50
Figure 3-4: An example of the system decomposition model.....	50
Figure 3-5: State transition diagram of a railway system from a train point of view.	51
Figure 3-6: An example of sequence and collaboration diagrams.....	51
Figure 3-7: BBN representation.....	55
Figure 3-8: An example of Fault and Event Tree	58
Figure 3-9: Fuzzy Patches.....	61
Figure 3-10: WeFA example.....	63
Figure 3-11: WeFA example (expanded).....	63
Figure 3-12: Basic structure of the Cause-Consequence Model.....	65
Figure 3-13: Overview of analysed methodologies and their applicability on the problem domain.	68
Figure 4-1: Outline structure and the argument presented in Chapter 4	70
Figure 4-2: Authorised Movement - Staff Responsible [Sequence & Collaboration diagram]	74
Figure 4-3: Core hazards models hierarchy	80
Figure 4-4: Model integration environment.....	83
Figure 4-6: State-space diagram.....	89
Figure 4-7: Axle Counter System	94
Figure 4-8: Parameterisation methodology.....	99
Figure 4-9: Concept of change.....	104
Figure 4-10: An example of the “System Architecture” diagram.....	110
Figure 4-11: Management Process.....	118
Figure 4-12: Railway System Model	124
Figure 5-1: Structure of chapter 5	129
Figure 6-1: Structure of chapter 6 and the argument in support of the claim that a newly developed process is sound and complete	139
Figure 6-2: “Hazard Universe”	141
Figure 6-3: Hazard attributes	145
Figure 6-4: Singerian inquiry system model.....	147
Figure 6-5: “Safety case derivation process system” within its environment.....	148
Figure 6-6: Generic safety case derivation process system	149
Figure 6-7: Example of reusable GSN pattern.....	152
Figure 6-8: Engineering Safety and Assurance Process	156
Figure 6-9: CSA and Risk Assessment Process.....	160
Figure 6-10: An example of System Definition.....	162
Figure 6-11: An example of the basic Process Model	162
Figure 6-12: Defence/Protection measures, Requirements and Quantified Requirements	174
Figure 6-13: Hazard Log Hierarchy.....	178
Figure 6-14: Hazard Log relationships	178
Figure 7-1: Structure of Chapter 7	184

Figure 7-2: Organisational structure of the Upgrade Programmes and two integration layers	190
Figure 7-3: Integrated safety management process.....	191
Figure 7-4: Integrated safety management process mapped onto organisational breakdown structure.....	192
Figure 7-5: VLUP Train Movement Accidents process model	201
Figure 7-6: Decomposition of process models	202
Figure 7-7: SSL System Level “Train Movement Accidents” process model.....	203
Figure 7-8: SSL “Immunisation Portfolio” Level “Train Movement Accidents” process model	204
Figure 7-9: ALARP Review Process	206
Figure 7-10: Restrictions identification and analysis process.....	211
Figure 7-11: Development of QRA models in support of staged project implementation	215
Figure 7-12: Development of Safety Arguments	234
Figure 7-13: Example of Safety Justification produced in support of the VLUP Testing of the new Train and Signalling system (DTG-R signalling system in overlay)	236
Figure 7-14: SSC mapped onto EN50129.....	242
Figure 7-15: VLUP GSN- Top level.....	242
Figure 7-16: Collision between trains GSN (VLUP System Safety Case)	243
Figure 7-17: Hierarchy of safety cases and justifications/evidences	245
Figure 7-18: SSL system level train movements accidents GSN	247
Figure 7-19: SSL project portfolio (subsystem) level train movements accidents GSN.....	248
Figure 7-20: SSL System safety argument document tree.....	249
Figure 7-21: Delivery management of the Safety Case	252
Figure 7-22: Typical programme of submissions.	253
Figure 7-23: Configurable data items	255
Figure 8-1: Structure of Chapter 8	260

List of tables:

Table 1-1: Acronyms and Abbreviations	18
Table 2-1: Principal engineering safety management activities.	32
Table 3-1: Hierarchy of real world complexity.....	38
Table 4-1: Consequence Groupings	79
Table 4-2: Sample of ERTMS study result data	84
Table 4-3: Category 0 Changes.....	106
Table 4-4: Category 1 Changes.....	106
Table 4-5: Category 2 Changes.....	107
Table 4-6: Category 3 Changes.....	108
Table 4-7 : Hazard identification Standard Guide words.....	112
Table 4-8: Characterisation of Change and Safety Benefits	113
Table 4-9: An example record from the CSA workshop.	113
Table 4-10: Railway system constituents classes and subclasses	123
Table 4-11: An example of interfaces description	125
Table 4-12: Example of high level safety requirements	126
Table 4-13: High level railway hazards	127
Table 4-14: Initial System Hazard Log sample (Core Hazards referenced to originating system interfaces)	127
Table 5-1: Comparison of facilities provided by different methodologies.....	136

Table 6-1: Hazard Log Elements and Relationships.....	180
Table 6-2: Configuration control and Journal data	181
Table 7-1: SSL Core Hazards definition.....	199
Table 7-2: VLU Train Movement Accident interfaces description	201
Table 7-3: SSL Train Movement Accident interfaces description.....	202
Table 7-4: Qualitative Ranking.....	207
Table 7-5: Risk Acceptability	207
Table 7-6: VLU Train Movement Accident-CSA Output Result.....	208
Table 7-7: SSL Train Movement Accident-System Level CSA Output Results	208
Table 7-8: SSL Train Movement Accident-Project Portfolio Level CSA Output Results	209
Table 7-9: Sample of the restrictions analysis outcome	213
Table 7-10: LU 2003 QRAs affected by changes to the railway introduced by VLU and SSL.....	217
Table 7-11: Model Element Data Sources Overview	222
Table 7-12: Total Risk (fatalities/yr).....	224
Table 7-13: Comparison of Initiating event frequencies.....	224
Table 7-14: Summary of Risk results.....	225
Table 7-15: Victoria line THRs.....	226
Table 7-16: Sample of QRA changes relevant to ISP	229
Table 7-17: Summary of Risk results.....	231
Table 7-18: An analysis of the signalling contribution to risk as calculated from the CSPVL	231
Table 7-19: Examples of Victoria Line related Safety Requirements	233
Table 7-20: Apportionment of responsibility for engineering safety management activities and delivery of evidence across the programme work packages.....	246
Table 7-21: Reporting - Change Safety Management process.....	254
Table 7-22: An example of the restriction's register record	258
Table 7-23: An example of the remit	259

CHAPTER 1: INTRODUCTION

1.1 Problem area

In engineering problems, detailed analyses of risk and its attributes can lead to significant benefits in safety performance and savings in time and money (e.g. analyses of essentially chaotic behaviour of winds lead to notable improvements in designs for buildings and bridges, not to mention benefits in weather forecasting, a classic example of a chaotic system).

Most of the existing processes and guidelines state what needs to be a result of the safety risk analysis, broadly outlining the expectations from each of the identified risks and depicted activities (listed later). Alternative methodologies exist, for some of the activities but not for all, each one invented and used in the context of different aspects of systems structure, behaviour and/or its emerging properties.

However, none of these amount to an integrated framework for the systems safety risk analysis and management.

For example, any sound analysis, including risk analysis, should be based on series of observations and measurements. The first stage of this activity, before the hazard identification can be carried out, should be to define a system to be analysed, including definition of the scope and context of the analysis and development of some form of system description. This preparation should also support identification of the experience and expertise of the participants of the hazard identification. Yet none of the guidelines provide any support in this area.

Furthermore, none of the processes depicted in the available literature, provide any guidance in relation to the monitoring of change of the system during its lifecycle and control of the impact of that change on the safety performance of the system.

These are just some of the shortcomings of existing processes and guidelines.

The scope of the research and this thesis includes engineering safety analysis and management applicable to any industry, but with the trial implementation being specific to the railway industry. The methodology aims to support systems safety analysis and identification of major contributors to safety risks and benefits, whilst safety and business decision making is supported through evaluation of different application solutions and mitigation measures. The methodology is supporting the holistic evaluation of safety risk and alternative solutions to a problem. Later in the thesis, this methodology is referred to as Engineering Safety and Assurance Process (ESAP).

1.2 Objectives and Aim of the Research

Society generally expects a level of safety from products and services and the current legislation (EU as well as UK) supports this view.

History demonstrates that safety failures can have significant societal costs, life or limb, monetary, environmental etc. Again, history shows that most accidents are avoidable.

Due to the above and other primary legislation we all have a 'Duty of Care' to the following groups:

- 1 Staff and Colleagues,
- 2 Passengers,
- 3 Members of the Public, and
- 4 The environment.

The complexity of modern projects and products demands the Systems approach to the analysis of Safety as an emerging property of the system, for a simple reason that with increased complexity of the systems produced by human kind our ability to comprehend the totality of the system without a structured methodical process is decreasing.

The objective of the research was to develop an innovative integrated methodology in support of safety risk assessment and management for engineering problems, in particular in support of introduction of large scale, novel and complex railway systems. However the developed process is generic and can be used in any industry or undertaking. The aim of the research was to contribute to decision-making and management practices involving safety risk. The research was carried out in three stages:

1. Research of existing industry practices and literature;
2. Application, testing and improvement of a selection of the existing processes on 4 real life projects. Development of new methodologies for risk assessment as part of this work;
3. Further development of an integrated innovative methodology, testing and implementation on a real life project.

Four projects were utilised as case studies for evaluation of existing methodologies and processes and initial development.

Once an outline framework had been created, utilising the existing methodologies on real life projects, the research focused on development of methodologies in support of the activities not catered for, or not sufficiently supported, by existing methodologies

and integrating these new methodologies with existing ones into a new process.

Three high level principles of analysis and management of safety risks must be respected and supported by adequate processes, because only by adhering to these principles one will be able to:

- 1 Ensure completeness of analysis;
- 2 Build a defensible argument in support of the final results (not forgetting that the choice based on the analysis may directly influence decisions potentially affecting human lives and costing millions).

These principles are:

- 1 Systematic Approach to the problem solving;
- 2 Holistic approach to the analysis;
- 3 Necessity of extensive use of Domain Specific Expertise.

After an initial literature research and following from experience of working on a number of railways related safety case development projects, a number of major steps have been identified as generic safety risk analysis and management process activities, as listed later. Processes and tools in support of missing, or insufficiently developed, stages were invented or further developed, and following that, an integrated process inclusive of all these steps was developed.

In summary, the result of the research project is a decision support methodology, which is already in use in support of making and managing decisions involving system safety risk and development of the safety cases on one of the most complex railway projects in this country, the upgrade of London Underground's Victoria Line (Lucic and Short, 2007) and Subsurface Lines (Metropolitan, District, Circle and Hammersmith & City and East London).

1.3 Structure of this thesis

This thesis is structured in 8 chapters as outlined by use of Goal Structuring Notation (GSN) in Figure 1-1 below. This research made significant use of the existing methodologies and processes, combining them with novel methodologies and processes (developed as part of this research) into a new general framework for safety risk analysis and management. GSN elements corresponding to novel processes and/or methodologies are indicated by red line outline. Later on, in the introduction to each chapter, discussion of the novel use of existing processes and methods has been indicated by blue and application of existing methods or processes within the new framework has been indicated by green.

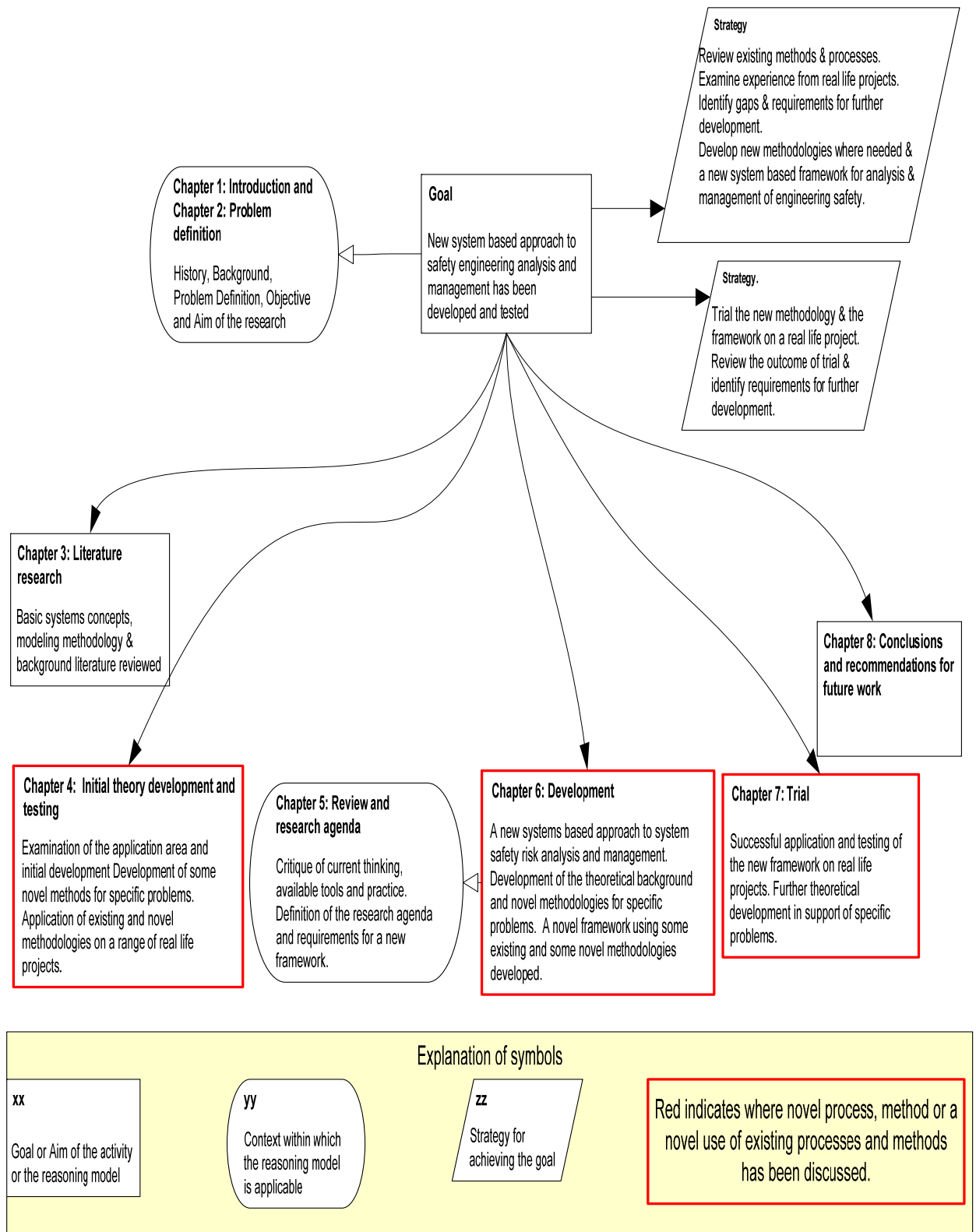


Figure 1-1: Overall Structure of the thesis

A more detailed outline of the logical argument of this thesis is provided within introduction for each of chapters 3, 4, 6 and 7 using Goal Structuring Notation.

The First chapter outlines the aim, objectives and scope of the research and thesis and presents the structure of the thesis. It also presents the more important definitions used later in the thesis.

The Second chapter portrays the history of the problem area and the background to the research and defines the problem area and research aims and objective.

The Third chapter presents the findings of the literature research and provides an overview of basic processes and tools for analysis, treatment and modelling of safety risk in engineering processes.

The Fourth chapter outlines the initial applied research areas and presents the findings of the early development. Four real life projects have been used as a vehicle for initial development and testing.

The Fifth chapter presents a critique of existing tools for analysis and management of safety risks and, using experience gained on the real life projects as outlined in the fourth chapter, sets out the agenda for the research.

The Sixth chapter develops the theoretical background of the basic concepts further and lays out a new system based framework for safety risk analysis and management.

The Seventh chapter presents the challenges, results and observations of application of the new framework on two real life projects.

The Eighth chapter concludes the findings of the research and outlines the requirements and direction of further research.

1.4 Definitions

The following are definitions of terms used throughout the thesis.

1. A system is an interconnection, organisation of objects that is embedded in a given environment (Karcianas, 2003). The System is the sum total of all constituent parts working together within a given environment to achieve a given purpose within a given time period. The totality of the system is a matter of perspective. It is not a fixed term, but can be defined arbitrarily;
2. System conceptualisation is a process of the development of the internal (constituent parts and their connections) and external (environment) system specification. A conceptual model should reflect knowledge about the application domain rather than about the implementation of the system (Milloti, 2004);
3. A Hazard is defined as an object, act or condition likely to lead to an accident;
4. An Accident is an unplanned, unintended event entailing loss;
5. A Consequence is the outcome of a hazard;
6. A Loss is defined as an undesirable, detrimental effect of an accident;
7. An opposite of the hazard is an Opportunity. This is an object, act or condition likely to lead to a gain;

8. A Gain is a desirable effect of the opportunity;
9. A Risk is a forecast for a future accident of a certain severity. An opposite of risk is reward;
10. A Risk Profile is a multi dimensional presentation of forecasts for future accidents, of certain severities, for a system. Additional dimensions introduced, may be time, space or some other relevant variable parameters.

1.5 Acronyms and Abbreviations

Acronym	Definition
AC	Alternating Current
ACC	Check in the MSCC docs
AGC	Standard for international Railway corridors
AGTC	Standard for international Railway corridors
ALARP	As Low As Reasonably Practicable
ALF	Algorithm File
ATO	Automatic Train Operation
ATP	Automatic Train Protection
AWS	Automatic Warning System
BBN	Bayesian Belief Network
BS	British Standards
BT	Bombardier Transportation
BTLUP	Bombardier Transportation London Underground Projects
CCS	Control Command and Signalling
CCTV	Closed Circuit Television
CENELEC	European Committee for Electrotechnical Standardization
CIS	Customer Information Systems
CM	Coded Manual (mode of operation of the new train)
CRMS	Cable Route Management System
CSA	Change Safety Analysis
CSDE	Correct Side Door Enable
CSP	Current Safety Performance
CSPSSL	Current Safety Performance SubSurface Lines
CSPVL	Current Safety Performance of Victoria Line
CSPVL	Current Safety Performance Victoria Line
DC	Direct Current
DRACAS	Defect Reporting, Analysis and Corrective Action System
DTG-R	Distance To Go – Radio (signalling system)
ECB	Engineering Change Board
ECR	Engineering Change Request
EDF	Energy Provider company
EEPL	EDF Energy Powerlink Limited
ELLCCR	Extra Low Loss Conductor Rail
EMC	ElectroMagnetic Compatibility
EMI	ElectroMagnetic Interference
EN	European Norm
ERTMS	European Railway Train Management System
ESAC	Engineering Safety and Assurance Case

Acronym	Definition
ESAP	Engineering Safety and Assurance Process
ESM	Engineering safety Management
ETCS	European Train Control System
EU	European Union
FET	Fault-Event Tree
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FRACAS	Failure Recording, Analysis and Corrective Action System
FSP	Final Safety Performance
FSPVL	Final Safety Performance Victoria Line
FT	Fault Tree
FTA	Fault Tree Analysis
FV	Fussel-Vesely (importance value)
GLEE	General Loss Estimation Engine
GPAD	General Parametric Data Set
GSN	Goal Structuring Notation
GUI	Graphical User Interface
HAZID	HaZard IDentificaiton
HAZOP	HAZard and OPerability (study)
HF	Human Factors
HMI	Human Machine Interfaces
HSE	Health and Safety Executive
ICSA	Initial Change Safety Analysis
ICSS	Initial Change Safety Analysis
IEEE	Institution of Electrical and Electronic Engineers
IET	Institution of Engineering and Technology
IHRG	Interdisciplinary Hazard review Group
INCA	Incident Capture and Analysis database
INCOSE	'International Council on Systems Engineering
ISA	Independent Safety Assessor
ISAE	Integrated Safety Assurance Environment
ISP	Interim Safety Performance
ISPVL	Interim Safety Performance Victoria Line
IT	Information Technology
LU	London Underground
LUL	London Underground Limited
LVAC	Low Voltage AC
MA	Manned Automatic (mode of operation of the new train)
MOP	Member of Public
MR	Metronet
MRBCV	Metronet Rail Bakerloo, Central and Victoria Line
MSCIP	Manchester South Capacity Improvement Project
NDUP	Neasden Depot Upgrade Project
OIDB	Objects and Interfaces DataBase
OPO TT CCTV	One Person Operation Track to Train
PAD	Parametric Data Set
PD	Position Detector
PDD	Project Definition Document
PFI	Private Finance Initiative
PHA	Preliminary Hazard Identification

Acronym	Definition
PKP	Polish railway authorities
PM	Protected Manual (mode of operation of the new train)
PMF	Project Management Framework
PPP	Public Private Partnership
PSR	Permanent Speed Restriction
PTI	Passenger Train Interface
QRA	Quantified Risk Assessment
RAM	Reliability, Availability and Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RBD	Reliability Block Diagrams
RM	Route Manual (mode of operation of the new train)
RSF	Right Side Failure
RSSB	Railway Safety and Standards Board
SAA	Station Area Accident
SCC	Service Control Centre
SCID	System Context and Interface Diagrams
SDO	Selective Door Opening Closed Circuit Television
SER	Signalling Equipment Room
SHL	System Hazard Log
SHWW	Sandbach/Wilmslow (geographical area of railway)
SIL	Safety Integrity Level
SIM	Check in the MSCC docs
SM	Slow Manual (mode of operation of the new train)
SSC	System Safety Case
SSL	Sub-Surface Lines
SSR	Sub Surface Railway
SUP	Subsurface Lines Upgrade Programme
TEN	Train European Network
THR	Tolerable Hazard Rate
TPWS	Train Protection and Warning System
TSI	Technical Specification for Interoperability
TSR	Temporary Speed Restriction
UNISIG	(European) Union Industry OF Signaling
VAF	Value of Avoiding a Ffatality
VL	Victoria Line
VLU	Victoria Line Upgrade
VLUP	Victoria Line Upgrade Programme
VPF	Value Preventing Fatality
WCMU	West Coast Management Unit
WRI	Wheel Rail Interface
WRSL	Westinghouse Rail Systems Limited
WSF	Wrong Side Failure

Table 1-1: Acronyms and Abbreviations

During one of many German air raids on Moscow in WW II, a distinguished Soviet professor of statistics showed up in his local air-raid shelter. He had never appeared there before. “There are seven million people in Moscow,” he used to say. “Why should I expect them to hit me?” His friends were astonished to see him and asked what had happened to change his mind. “Look,” he explained, “there are seven million people in Moscow and one elephant. Last night they got the elephant.”

CHAPTER 2: PROBLEM DEFINITION

2.1 Chapter Introduction

Findings of the research of the history of the perception and understanding of uncertainty and risk and investigation of the existing theoretical and analytical framework in relation to treatment of safety in engineering are presented in this chapter.

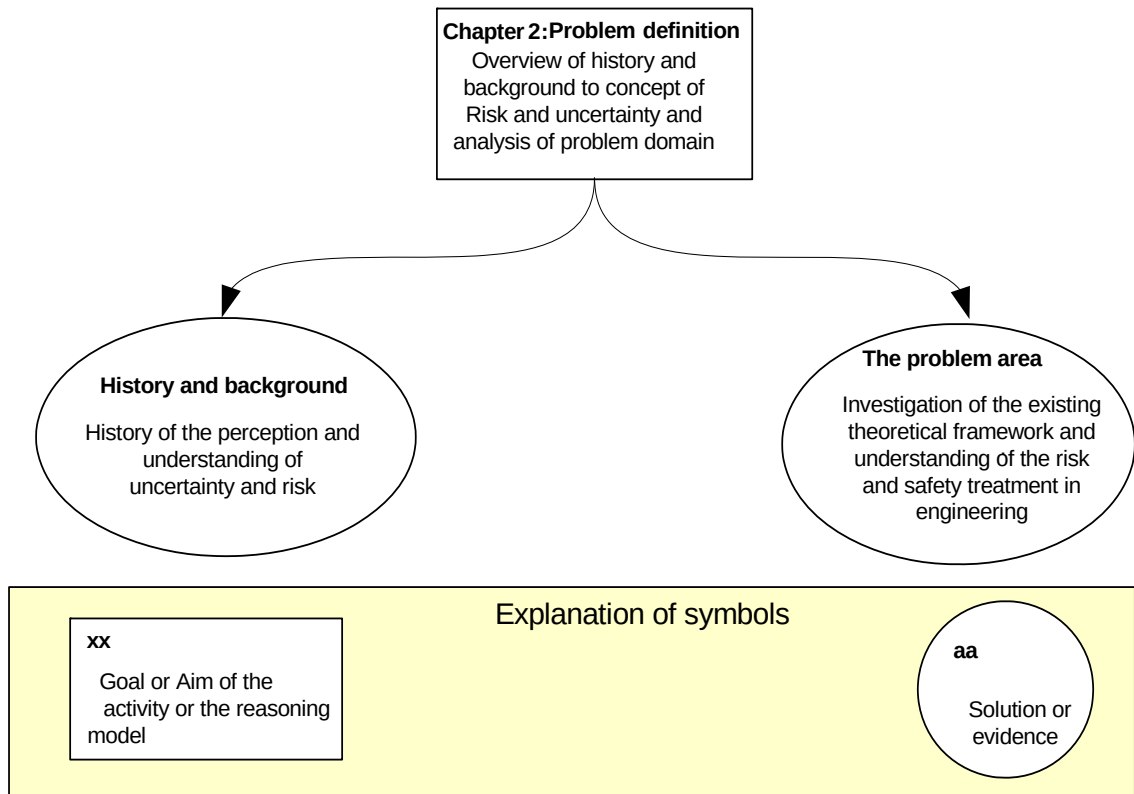


Figure 2-1: Structure of Chapter 2

2.2 History and Background (Waldrop, 1992), (Bernstein, 1996)

Everyday experience is rich with uncertainties and (most of the time unconscious) risk analysis. The treatment of risks that we are performing everyday familiarises us with the subject. Impulses of nature, inaccuracy of our senses and tools, new technologies and foolishness of human beings all complement to the level of uncertainty. Early in life we learn to rely on a series of intuitive models of common situations, outcomes of which depend on unknown factors.

This ability of our mind for complex statistical analysis is often sufficient, but still situations where one could benefit from more sophisticated treatment of issues are many.

Unfortunately, ignorance about the scientific advances in this field, as well as far too much confidence into intuition prevents one from gaining advantage by using powerful

and, more often than not, simple sets of tools provided by probability, statistics and the sciences of dynamical systems and stochastic processes.

The word “RISK” evolves from “*RISKARE*”, the Latin for “TO DARE”. Amusingly, if we follow this logic, risk is a choice we make, not a fate.

To explain the creation of universe, Greek mythology used a game of dice. Zeus, Poseidon and Hades rolled the dice for the universe. Zeus won the heavens, Poseidon the seas and Hades ended up with hell, becoming master of underworld.

Regardless of the fact that risk taking has been implanted in our existence from the beginning, development of the science of risk and of statistics has been somehow delayed when compared with other sciences. Astronomy, medicine, philosophy, physics and mathematics all have foundations in great ancient cultures of Egyptian, Persian, Greek, Roman and Chinese civilisations. On the other hand, the first serious study of risk happened during the Renaissance (Bernstein, 1996).

There are two main reasons for this long delay (Stermann, 2000).

Firstly, for too long the belief was that the future is shaped by the forces of gods and that human beings are not actively involved in shaping nature and consequently the future. Until the Renaissance, the future was regarded as an already written book. Fate was determined by the sins of the past and there was nothing human beings could do to change it. People’s perception of the future was passive.

Depending on different religions and cultures, for people of ancient times, the future was either a matter of luck or the result of closeness of their sins to their god’s wish. For thousands of years people’s lives were very static and the most important variable influencing their lives was the weather and other unforeseen natural elements.

The second reason is a fact that the purpose of the numbering system at the time was to satisfy only the needs for recording of measurements but not for the calculations. Then Hindus developed the numbering system we use today, in about 500ad. Arabs adopted this number system and spread it across the western civilisation through Spain. The centrepiece of the Hindu-Arabic system was the invention of zero. This supported rapid development of calculus and algebra.

Modern mathematics is based on the work of Aristotle and the philosophers who preceded him. Their work has culminated in several “Laws of Thought”, sets of theories supporting concise and systematic approach to logic and later mathematics. One of the

most important laws was the “Law of Excluded Middle”. The law stated that every proposition must be either True or False. Every statement is True or False, 1 or 0.

Nevertheless, the ancient Greeks gave a thought to probability theory. Socrates defines a meaning of Greek word “Eikos” (Εἰκος) as “likeness to truth”, and reveals an important phenomenon, “likeness to truth is not the same thing as the truth”. Plato in his work indicated that there was a third region, between True and False, a space where nothing was completely True or False, but that was as far as the ancient Greeks went.

Only when the civilisation reached a phase of progress that required from humans to take charge of their own existence in order to secure further advance and control ever increasing pace of change, the need for prediction of future became necessity. During the renaissance the pace of social, cultural and environmental change increased dramatically. People could not afford to be at mercy of fate any more, they could no longer remain passive in the face of unknown future.

The intensifying pace of change and competition all around, forced transformation of mysticism into science and logic and the human race made the first attempt to liberate itself from self-imposed limitations.

The mathematical foundation of the concept of risk, the theory of probability, is a result of joint efforts of two great minds of the time, Blaise Pascal, a French mathematician and Pierre de Fermat a lawyer and mathematician, who published their work in 1654. At about the same time, Antoine Arnauld, a theologian, was first to state that “Fear of harm ought to be proportional not merely to the gravity of the harm, but also to the probability of the event”, or in other word, only the combination of likelihood of outcome and value of outcome should influence a decision.

Methods of statistical sampling and the Law of Large Numbers were invented in 1703 by Jacob Bernoulli. Abraham de Moivre discovered the concept and structure of normal distribution in 1730. Around the same time Daniel Bernoulli defined the systematic process by which people make choices and decisions. Thomas Bayes discovered a way to make better-informed decisions by mathematically blending new information into old information, about 1750. In 1875, Francis Galton, discovered regression to the mean and Harry Markowitz demonstrated mathematically why diversification is desirable in 1952.

Everyone knows that “uncertainty” affects a project manager about to define the price for the contract, an engineer about to sign replacement approval for piece of equipment

or a trespasser taking that first dangerous step. The concept of hazard comes about due to our recognition of future uncertainty, our inability to know what the future will bring in response to a given action today.

Uncertainty implies that a given action, or non-action, has more than one possible outcome.

‘Uncertainty’ in everyday use denotes unknown factors that influence outcomes of observed developments. To analyse these more efficiently, one needs to consider several fundamentally different types of uncertainty (Waldrop, 1992), (Checkland, 1984), (Bhatnagar and Kanai, 1991).

The first category can be described in an *Objective Probability Framework*. This is suitable, for example in a Quality Control Methods context, where we monitor sample and ensure that required standards are met. We also frequently study the likely impact of changes in systems to see how we might improve efficiency or reduce costs.

In the second category we will include all the uncertainties that arise at a fundamental level, that is the uncertainties that arise because parameters of the problem are non-computable or are fundamentally non-deterministic. These kinds of problems are found most notably in the theory of computation and in quantum mechanics¹ respectively.

Some problems of uncertainty may not be easily classified in either of the two categories, possessing the elements from each. We are able to predict, with significant accuracy safe operating limits for railway system. Here we deal with uncertainties of the first kind. Still, acts of terrorism, human error or foolishness, unpredictable nature of some mechanical failures all introduce uncertainties of second category to our analysis. The third type of uncertainties are introduced as a consequence of our ignorance of background theory, either conscientiously because it is impractical or unjustifiably costly to include these considerations into calculations, or as a result of unawareness of all parameters or laws governing the outcome. In these situations one chooses to treat the problem as one of the first two types.

The third kind of uncertainty deals with potential hazards and exploring the unknown. It is often a subjective rather than objective exercise and our perceptions are an integral part of our assessment. The second type we will use to classify all the problems where uncertainty occurs as a result of essential difficulty in calculating results of a

¹ These two types of problems can be argued to be formulations of the latter (quantum mechanical) on different levels of complexity, i.e. the fact that non-computable problems exist may well be a direct consequence of the existence of non-deterministic ones. This is since quantum mechanics is intended to be description of nature at the most fundamental level.

deterministic process. This includes chaotic systems (ones in which the outcome is deterministically dependent on initial conditions, but is also extremely sensitive to their change, making it practically impossible to predict it) and problems in which computing a solution is probably unfeasible.

Problems of this class can be often met in a number of engineering fields, included are certain behaviours of a realistic pendulum, the rate at which a fluid is dripping from a tap or a problem of calculating most efficient ways of traversing complex networks as a model of routes taken by electric shocks and so on.

In technical applications uncertainty can be categorised in three classes (Fenton and Hill, 1993):

1. Incompleteness of relevant knowledge;
2. Uncertainty of knowledge;
3. Imprecision of knowledge.

In most situations the relevant knowledge is incomplete. In these cases one is faced with the problem of deciding which one of potentially many different solutions is the true one.

More often than not we are not sure that information we have is the absolute truth.

Uncertainty of data relates to observations of nature or society. The observer is uncertain about what has actually been observed or about the measurements taken.

Measurement and sampling are two sources of data uncertainty. There is always some uncertainty in any measurement, because of limited precision of the measuring device. This can usually be determined from the characteristics of the device and by repeated sampling and statistical characterisation.

Imprecision of knowledge or rule uncertainty relates to reasoning about the observations. The observer is doubtful about the conclusions drawn from the data.

When considering systems, as defined in the section “Definitions” (1.4), the uncertainty is related to incompleteness, uncertainty and imprecision of knowledge about systems constituents or objects that make up a system, the connections between these objects, organisation of objects, the system topology, the system environment and interactions between the system and its environment.

Most commonly, practical problems have uncertain factors of more than one type. In real life the number of parameters influencing outcomes of all but the most trivial of

problems are so numerous that we usually decide to ignore most of them and describe them as ‘uncertainty’ in the problem, regardless of the type to which they belong.

2.3 The Problem Area – detailed analysis

“Fear of harm ought to be proportional not merely to the gravity of the harm, but also to the probability of the event” (La logique, ou l’art de penser (Logic, or the art of thinking); 1662 – Antoine Arnauld as cited in (Bernstein, 1996)). The safety is defined as freedom from harm.

Before it is possible to proceed further, it is important to describe our world from the point of view of the person dealing with the uncertainty:

1. Our world is speculative. (“Our knowledge of the way things work, in society or in nature, comes trailing clouds of vagueness. Vast ills have followed a belief in certainty”.(Kenneth Arrow as cited in (Bernstein, 1996)));
2. Perfection implies repetition of assessment, estimation, calculation, evaluation, analysis and computation (Fenton and Hill, 1993);
3. Precision is a measure of vicinity of the measurement to the correct value (Fenton and Hill, 1993);
4. Both, the gauging of the tools used for measurements as well as the dimensions measured fluctuate constantly (Fenton and Hill, 1993);
5. A degree of required precision, or in other words allowed level of uncertainty, depends on criticality of the measure to be used (Hessami, 1999b);
6. Risk is directly proportional to uncertainty, the lesser the uncertainty, the lower the risk. Furthermore the more we know about the world the lesser is uncertainty;
7. Risk and time are interrelated. Without time there is no risk. The risk is only relevant in relation to future. Passage of time transforms the risk and its nature.

Therefore, in the simplified sense, every action is “uncertain”, from crossing the street to building a railway system.

The term “hazard” is usually reserved, however, for situations where the range of possible outcomes to a given action is in some way significant. A significant outcome is a very loose definition, but in truth it is a highly flexible concept. The level of significance varies depending on the level of gain and human perception of acceptable uncertainty.

Common actions like crossing the street are usually not “hazardous” while building a railway system can involve significant uncertainty. Somewhere in between, actions

pass from being non-hazardous to hazardous. This distinction, although vague, is important; if one judges that a situation is hazardous, the level of hazard becomes one criterion for deciding what course of action should be pursued.

This research focused on the treatment of safety risks in railways. Existing methodologies for assessment and management of the safety risk on railways are mostly empirical and have been developed out of a need to satisfy the regulatory requirements and in response to a number of major accidents. Almost all of these processes and methodologies have been developed in support of approvals of specific products or very simple systems and do not add up to a holistic coherent methodology suited for analysis of modern, complex systems, involving many vastly different constituents (software, hardware, people, products developed in different parts of the world, etc.). Complexities of modern railway projects necessitate new approach to risk analysis and management.

At the outset, the focus of the research was on the organisation of the family of existing system analysis methodologies into a coherent, heterogeneous methodology.

Relationships between different methodologies and their properties were investigated seeking to define the rules for embedding of models into a hierarchical nest and relating their emergent properties.

Once an outline framework has been created utilising the existing methodologies on real life projects, the research focused on development of methodologies in support of the activities not catered for, or not sufficiently supported by, existing methodologies and integrating these new methodologies with existing ones into a new process.

In general any activity is undertaken (Hessami, 1999b) when there is a perception that the balance between the potential loss and the potential gain is such that it is worth pursuing the activity further. At that point, some form of risk analysis becomes viable. Most authors define the risk as a combination of loss and frequency or probability of occurrence. However (Hessami, 1999b) other parameters define the risk as well:

1. Nature of the consequent loss;
2. Severity of the loss;
3. The nature of initiating hazard;
4. Affected party;
5. Probability or frequency of occurrence of the consequence.

The detailed analyses of these can be very profitable. This, ‘more detailed analysis’ can extend to several levels to include above mentioned subjects of study, but the most common, as well as the simplest, is the one covered by probability and statistics.

In engineering problems, detailed analyses of risk and its attributes can lead to significant savings in time and money (e.g. analyses of essentially chaotic behaviour of winds lead to notable improvements in designs of buildings and bridges, not to mention benefits of weather forecasting, a classic example of a chaotic system).

During the research three high level principles of analysis of safety risks have been identified that must be respected and supported by adequate processes, because only by adhering to these principles one will be able to:

1. Ensure completeness of analysis;
2. Build a defensible argument in support of the final results (not forgetting that the choice based on the analysis may directly influence decisions potentially affecting human lives and costing millions).

The first principle is that of Systematic Approach to problem solving. Planning the safety activities, documenting the work and enforcing rigorous configuration control of all important documents and data is the paramount. For different problems, different tools and techniques may be appropriate to ensure completeness of analysis.

Holistic approach to the analysis is the second principle. From a systems perspective, safety is an emerging property of a system. When analysing the system, all elements of the system must always be taken into consideration (software, hardware, human factors, socio-political influences and environmental issues, to mention some), throughout the life cycle of the system. The information about the analysed system should be reliable and complete.

The starting point of the safety management process is most of the time taken to be the risk assessment. More often than not, when doing risk assessment and analysis, the knowledge of experts in the particular field is exploited. Nowadays even apparently simple systems consist of parts designed by experts of different disciplines: electronics, mechanical, software and ergonomics come to mind first. On top of this, modern products are used in the wide variety of applications with different operational conditions.

Finally, the third principle of safety risk assessment is necessity of extensive use of Domain Specific Expertise.

The systematic risk based approach to any undertaking has been developed within Railtrack PLC (now Network Rail) and has become a nationwide Engineering Safety Management guidance adopted by LUL and the whole of UK railways. Following are the risk assessment principles (RSSB, 2007):

1. Hazard Identification;
2. Causal Analysis;
3. Consequence analysis;
4. Loss analysis;
5. Options analysis;
6. Impact analysis;
7. Demonstration of compliance with the bench mark.

The following diagram depicts the above mentioned process in more detail.

The 7 Stage Process assumes that the system is already well understood and defined.

Several approaches to the hazard identification exist (for example guidance in (Civil Aviation Authority, 2006)), but the most common is in a form of a structured brainstorm where focus of the session is secured by consideration of the keywords, such as NOT, LATE, EARLY, ALSO, etc, on the problem domain.

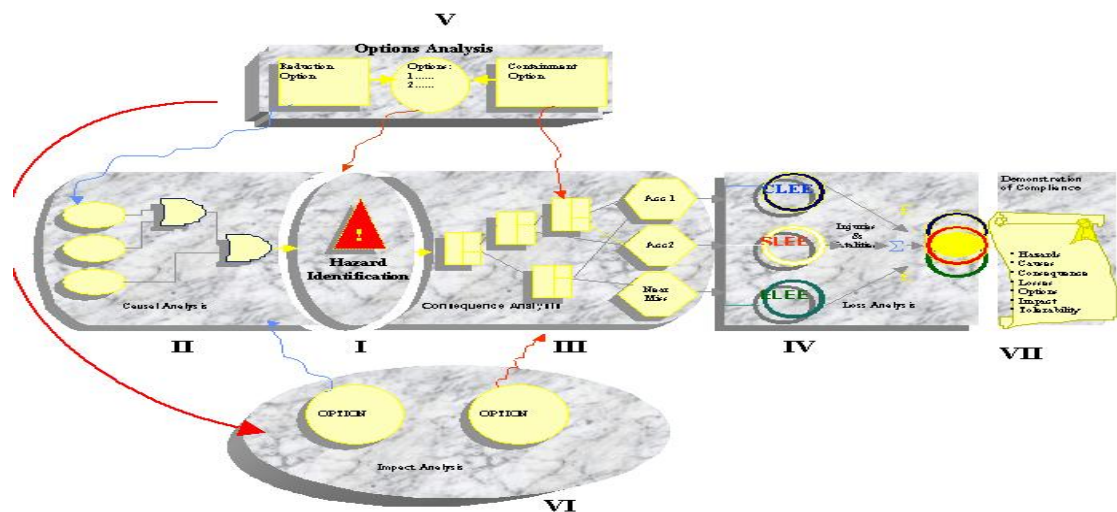


Figure 2-2: 7 Stage Process

The result of **hazard identification** is a linear mass of information. Hazards are defined on their own without any reference to potential relations and dependencies to other hazards. It would be extremely difficult to analyse each of these hazards on its own and to simultaneously ensure that all interactions between different hazards and common dependencies of multiple hazards have been systematically analysed.

The final outcome of the analysis must not include any double counting or exclude any of the constituents of the system.

This is why grouping of hazards of the same origin into larger entities referred to as core hazards, should be performed as the next step of analysis.

On-line capture, using the projector and the laptop, of information during hazard identification session (and any other group workshop) has been proven to be extremely effective. The main benefit is that the panel can agree (or argue about, which is more usual) the final version of information to be captured (wording of the hazard and its consequences and mitigations, in case of hazard identification). Hazard identification session must be well structured and planned. Participants must be allowed to express their opinion and encouraged to take an active part in the session.

Domain Competence Requirements are determined by the problem under consideration. Care must be taken to ensure that expertise, related to all aspects of the problem area, is comprehensively incorporated into a study throughout the process. In order to secure as comprehensive as possible source of data and ideas, care should be taken to form groups with wide range of expertise.

The aim of the **causal analysis** is to identify all the events/causes, and all the intermediate conditions which lead to a hazardous condition.

Consequence analysis involves establishing the intermediate conditions and final consequences that may arise from a hazard. It involves bottom-up assessment of each hazard and is focused on the post hazard horizon. At each intermediate state existing defences against potential escalation should be identified. The defence may be equipment, procedure or circumstance. The sequence of the identified intermediate conditions is termed “the hazard development scenario”. Final consequences fit into one of the following categories: predominantly safety related consequence, predominantly commercial consequence, predominantly environmental consequence, broadly safe condition.

Loss estimation is the process of estimating the losses that result from an accident or incident. These losses may be of three kinds: commercial, safety and environmental. Under each of these categories there are a number of ways in which losses may be incurred. These are termed loss mechanisms.

Each of the loss mechanisms should be considered. Therefore the first task is to identify each of the relevant loss mechanisms for a particular incident.

Having identified the relevant loss mechanisms it is then necessary to estimate the associated losses. It is useful to rank the loss mechanisms in order of estimated magnitude, so that it is apparent if the losses are primarily commercial, safety or environmental.

Safety losses in terms of injuries or equivalent fatalities are notoriously difficult to estimate.

For major accidents, there is (fortunately) not a large enough sample for results to be statistically significant, so often it is necessary to make a (conservative) estimate.

In order to normalise the units of loss (commercial, safety and environmental) and enable comparison of risks and gains, the safety loss is often converted into financial losses. In UK the Health and Safety Executive's (HSE) Value for Preventing a Fatality (VPF) is often used. This is £0.99 million for one or less equivalent fatalities and £3.12 million for accidents involving more than one equivalent fatality, where 1 equivalent fatality = 1 fatality or 10 major injuries or 200 minor injuries. Safety losses are, by convention expressed in terms of Potential Equivalent Fatalities per annum.

Options analysis is aimed at identification of potential reliability improvements and damage containment. This stage of the process is a creative phase employing the empirical knowledge and inspiring elicitation techniques. For each identified option following information should be elicited:

1. Costs;
2. Loss Prevention Capability;
3. Resource & Competency Requirements;
4. Time-Scales;
5. Uncertainty & Dependency;
6. Impact on Other Loss Dimensions.

The systematic assessment of overall effect of each identified option on the potential risks is referred to as the impact analysis.

Impact of each identified option on the reduction or containment of identified risks should be assessed.

In case of safety risk, the demonstration of compliance in the UK involves comparison of the total individual risk arising from the malfunction of the system against the

industry benchmark as a minimum required safety performance and against the investment required to improve the system further.

The first part of this stage is related to the maximum acceptable risk exposure which is in UK set by HSE (Health and Safety Executive, 2009).

The second part of this stage is related to the foundation of the assurance that everything reasonable has been done in order to minimise the risk arising from the malfunction of the system. Each of the identified options should be assessed, the improvement that option can bring if implemented against the cost of the option implementation as well as other parameters defining the options listed above.

The risk assessment can be qualitative or quantitative. Once all the reasonably practicable options have been implemented it can be demonstrated that the safety risk arising from the malfunction of the system is acceptable.

Current practice in the UK demands demonstration of compliance with the As Low As Reasonably Practicable (ALARP) principle for any undertaking. This demonstration is typically structured in the form of a Safety Case.

Very similar approach to the safety management is discussed in many other papers and standards ((SAMRAIL, 2004) to mention one) but all of these are very similar to the “7 stage process” and to avoid duplication these will not be discussed here.

The extension of the “7 stage process” is the rational approach to risk assessment, inclusive of both, rewards and risks of the enterprise, the benefits and the detriments brought by the system. Following this logic (Hessami, 1999a), if a hazard is the precursor to risk, the opportunity is the precursor to reward. Therefore, in order to ensure that the totality of the system has been analysed (for safety) it is necessary to assess the benefits of the system as well as risks.

Safety assurance of a system covering the complete generic lifecycle could be split into two phases (CENELEC 1998), (CENELEC 2003), (Hessami, 1999b), (RSSB, 2007):

1. Safety Engineering, covering design, development and realisation of the system;
2. Safety Management, covering deployment, maintenance, retrofit and decommissioning.

Generic lifecycle phase	Principal ESM activities
Concept and feasibility	Preliminary hazard identification
	Establish the hazard log
	Define the preliminary safety plan

Generic lifecycle phase	Principal ESM activities
Requirements definition	Hazard Analysis (and revisiting of hazard identification)
	Risk Assessment
	Establish safety requirements
	Define full safety plan
Design	Risk Assessment
	Safety Audit
Implementation	Risk Assessment
	Safety case
Installation and handover	Safety Assessment
	Safety Endorsement
	Transfer of safety responsibilities to the user
Operations and Maintenance	Update the Hazard Log and safety case
Decommissioning and Disposal	Update the Hazard Log and safety case

Table 2-1: Principal engineering safety management activities.

The safety engineering phase correlates with the pre operational phases whilst the safety management phase correlates with the application and maintenance aspects of the system lifecycle. Although these two phases are interconnected and overlap in many aspects, the methodology for management of risks and the tools and processes supporting the risk management are quite different.

During the safety engineering phase the focus of safety risk management is on provision of a system with the potential to provide safe performance. The focus of the safety management phase is to realise that potential. As part of the railways Engineering Safety Management (ESM) guide (RSSB, 2007) a detailed breakdown of activities, related to the system life cycle, required to ensure a safe delivery and use of a system is provided.

Most of the existing processes and guidelines state what needs to be a result of the safety risk analysis, broadly outlining the expectations from each of the above listed and depicted activities. Alternative methodologies exist, for some of the activities but not for all, each one invented and used in the context of different aspects of systems structure, behaviour and/or its emerging properties.

However, none of these amounts to an integrated framework for the systems safety risk analysis and management. Many examples of failure to assure the clients and relevant authorities (Her Majesty Railway Inspectorate, for example) of satisfactory safety performance of the system exist in the railway industry. To mention one example, failure to demonstrate satisfactory safety performance of a novel signalling system

(upgrade of a railway junction on a main railway line) led to two year long delays in implementation and a mounting cost (some estimates are that the final cost of the system will be two orders of magnitude higher than original tendered cost).

There are also examples of the opposite, where grossly underestimated cost of an option may have caused delay to the implementation of potentially almost equally efficient option. Following from the investigation into Clapham junction train accident in 1988 (35 fatalities and 69 major injuries) led by Sir Antony Hidden, a recommendation was made that the Automatic Train Protection system should be fully implemented within 5 years of selecting a specific type of the system, with high priority being given to densely trafficked lines (Department of Transport, 1989), (Health & Safety Commission, 1998). Subsequently the recommendations from Hidden enquiry were reinforced in particular in the report into an accident at Cowden in 1994. However, the state of development of technology and consequently, the high cost of development and implementation at the time when recommendations were made, prevented the implementation of recommendations within the timescales suggested by enquiries. Furthermore, spiralling cost of failed implementation of the modern ATC (ERTMS/TCS) system along West Coast Main Line was a major cause of demise of Network Rail. During late 90s (Health & Safety Commission, 1998) TPWS was identified as a reasonable practicable minimum requirement. The rollout of this system has been successfully initiated in parallel with conclusion that introduction of ATP system may not be justified on the bases of cost until the technology developments advance further.

If at the time of the first recommendation more measured view was taken of the whole life cost of ATP systems, TPWS could have been proposed as a pragmatic way forward much and implemented across the most critical parts of the network much earlier, thus potentially preventing some of the later accidents. This is an example of where the cost of safety must be analysed systematically and carefully, taking into account full life cycle cost, so to support the justifiable decision making.

Furthermore, in different industries significantly different levels of investment are expected on health and safety. Thomas and Stupples (Thomas and Stupples, 2006) have devised a new approach to appraisal of reasonable practicability as part of the options and impact analysis. The J-value is the ratio of the actual spend and the maximum reasonable spend which in turn is a function of life expectancy, average income and work life balance. Number of case studies has been undertaken, including an assessment of J-value related to implementation of TPWS and ERTMS ATP systems. For both

(TPWS and ERTMS ATP) the J-value was found to be greater than unity, indicating that both are costing more than what it should. J-value for TPWS was found to be between 3.8 and 11.3, and for ERTMS ATP between 38 and 132, strongly supporting the argument that ATP systems are far too expensive for the realised benefit.

All of this must be taken into account when options and impact analysis are undertaken.

The root cause of the failure to undertake the complete, holistic analysis is twofold:

1. Lack of understanding of the complexities involved in development of modern systems;
2. None-existence of a holistic methodology, and the process supporting it, throughout the lifecycle safety analysis and management.

As discussed later in this thesis, the complexity of modern projects and products demands the Systems approach to the analysis of Safety as an emerging property of the system, for a simple reason that with increased complexity of the systems produced by human kind our ability to comprehend the totality of the system without a structured methodical process is decreasing.

2.4 Chapter Conclusion

In this chapter the author outlined the background and the history of the human perception of risk. Since risk is an abstract, almost philosophical concept, this initial research and discussion was necessary to set out the scene for further research.

Following from that, the author investigated the problem domain further, aiming to plot out direction for the research. The author identified the gaps in existing knowledge and application and outlined the high level requirements that a future framework must satisfy. This work is presented in this chapter as well.

CHAPTER 3: BASIC SYSTEMS CONCEPT, MODELLING METHODOLOGY AND BACKGROUND LITERATURE

3.1 Chapter Introduction

The findings of the initial literature research are presented here. The research was conducted in two specific areas (as indicated by Figure 3-1 below), research of systems theory relevant to safety engineering and management and research of the tools and methods used for specific engineering safety problems.

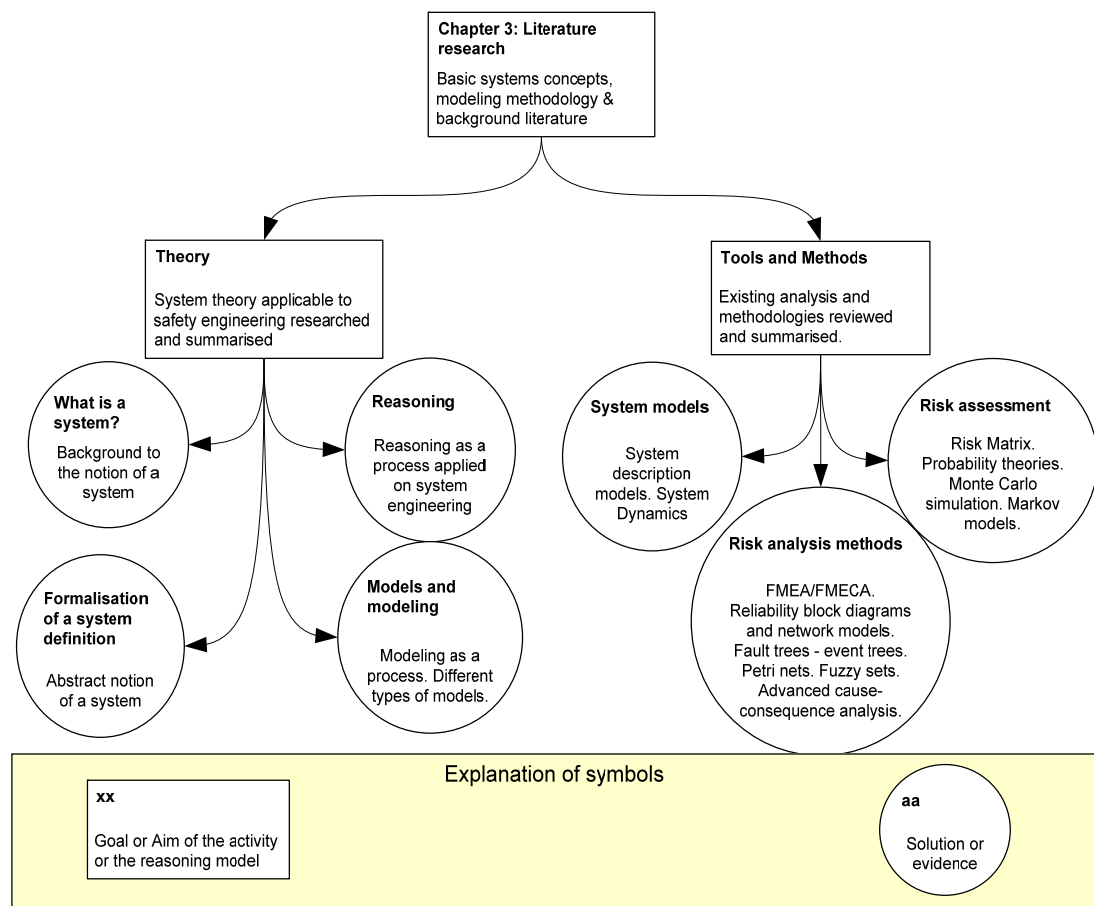


Figure 3-1: Structure of chapter 3

3.2 Background to the notion of the system

There are many different definitions of a system.

Benjamin and Wolter (Blanchard and Fabrycky, 1998) conclude that a system is assemblage or combination of elements or parts forming a complex or unitary whole, such as a river system or a transportation system; any assemblage or set of correlated members, such as a system of currency; an ordered and comprehensive assemblage of

facts, principles or doctrines in a particular field of knowledge or thought, such as a system of philosophy; a coordinated body of methods or a complex scheme or plan of procedure, such as a system of organisation and management; any regular or special method of plan of procedure, such as a system of marking, numbering or measuring. A system is characterised by unity, functional relationship and a useful purpose.

A system is a set of interrelated constituents working together toward some common objective or purpose. The set of constituents has the following properties:

1. The properties and behaviour of each constituent of the set have effect on the properties and behaviour of the set as a whole;
2. The properties and behaviour of each constituent of the set depend on the properties and behaviour of at least one other constituent in the set.
3. Each possible subset of constituents has the two properties listed previously; the constituents cannot be divided into independent subsets.

A system is more than a sum of its parts. However, the constituents of a system may themselves be systems, and every system may be part of a larger system in a hierarchy.

Another, more pragmatic definition of a system comes from the internal document of an engineering company (Blanchard and Fabrycky, 1998): “A system is the interacting combination of equipment, people and processes designed to accomplish a defined objective. The environment is that part of the rest of the world that a system interacts with.”

As a last example the following definition of a system is given by Norman Fenton and Gillian Hill (Fenton and Hill, 1993): “A system is an assembly of constituents connected together in an organised way and separated from its environment by a boundary. This organised assembly has an observable purpose, which is characterised in terms of how it transforms inputs from the environment into outputs to the environment. In order for systems to function effectively they generally require some kind of control mechanism. This monitors external behaviour, providing feedback and enforcing changes to the system where necessary.”

In his book (Waring, 1996) Alan Waring defines the system in a similar manner as the above mentioned authors.

Any system is characterised by its emerging properties, the properties that are an outcome of the joined act of the system parts.

The system constituents (Blanchard and Fabrycky, 1998) are the operating parts of a system consisting of input, process, and output. Each system constituent may assume a variety of values to describe a system state as set by some control action and one or more restrictions.

Attributes are the properties of discernible manifestations of the constituents of a system. These attributes characterise the system. Relationships are the links between constituents and attributes.

A purposeful action performed by a system is its function.

A system is defined by its boundary or scope. Everything that is outside the boundary is considered to be the environment. No system is completely isolated from its environment. Material, energy, and/or information are passing through the boundaries as input to the system. In reverse the material, energy, and/or information that is passing through the boundaries from the system is referred to as output. That which enters the system as one form and exits from system in another form is known as throughput.

Every system is made up of constituents, and in turn any constituent may be broken down into smaller constituents. If two hierarchical levels are involved in a given system, the lower is conventionally called subsystem.

A subsystem (Fenton and Hill, 1993) is a system in its own right that is contained within some other system. Most real systems are so complex that the only way one can understand them is to understand their recursive structure by thinking in terms of their simpler, interconnected subsystems.

If these systems are themselves too complex most often one again thinks in terms of their subsystems. This process of looking for simpler subsystems within subsystems is repeated as many times as necessary. The process is called top down decomposition and it gives rise to notion of levels of abstraction. It is the only known means of analysing complex systems.

Some authors have made an attempt to classify systems.

Benjamin and Wolter (Blanchard and Fabrycky, 1998) introduce the following classification:

1. Natural and human made systems;
2. Physical and conceptual systems;
3. Static and dynamic systems;

4. Closed and open systems.

Checkland (Checkland, 1984) supports the idea of 9 levels hierarchy of real world complexity:

Level	Characteristic	Examples	Relevant disciplines
Structures, frameworks	Static	Crystal structures, bridges.	Description, verbal or pictorial in any discipline.
Clock-works	Predetermined motion – equilibrium	Clock, machines, the solar system.	Physics, classical natural science.
Control mechanisms	Closed loop control	Thermostats.	Control theory, cybernetics.
Open Systems	Structurally self-maintaining	Flames, biological cells.	Theory of metabolism (information theory)
Lower organisms	Organised whole with functional parts, blue printed growth, reproduction	Plants.	Botany.
Animals	A brain to guide total behaviour, ability to learn	Birds and beasts.	Zoology.
Man	Self-consciousness, knowledge of knowledge, symbolic language.	Human beings.	Biology, psychology.
Socio-cultural systems	Roles, communication, transmission of values	Families, clubs, nations.	History, sociology, anthropology, behavioural science.
Transcendental systems	Inescapable unknowables	The idea of god.	

Table 3-1: Hierarchy of real world complexity

the authors suggest the use of above classifications to aid choice of a method for system analysis. One other categorisation of complexity defines two types, essential and accidental complexity.

Essential complexity, as named, is in the essence of the system. It is an inherent part of a system and cannot be eliminated but only minimised. Accidental complexity is not the “natural” attribute of the system but is a consequence of an accident. This type of complexity can be eliminated. The following systems analysis methodologies are suggested (Checkland, 1984), (Waring, 1996), (Blanchard and Fabrycky, 1998):

A. Hard system thinking including following steps:

1. Doing the groundwork;
2. Gaining awareness and understanding of the perceived problem;
3. Establishing overall goals and set of objectives;
4. Finding ways to reach objectives;
5. Devising assessment measures;
6. Modelling;

7. Evaluation;
8. Making a choice;
9. Implementation.

B. Soft system thinking including following steps:

1. Data collection;
2. Analysis;
3. Relevant systems and root definitions;
4. Conceptual modelling;
5. Comparisons to provide debating agenda;
6. Discussing the agenda with the actors;
7. Action for change;

C. Systems failure thinking including following steps:

1. Describing the failure situation;
2. Comparison with paradigms;
3. What do comparisons mean;
4. Learning.

With aspiration to unite the different approaches, soft, hard and systems failure systems thinking, the author will introduce a new generic definition of a system.

3.3 The abstract notion of the system

A system is a collection of interconnected, organised parts, embedded in the environment, that forms a whole which exhibits some new properties that none of the constituents possess on their own.

From a point of view of a high level safety analysis strategy, if the definition of a system given above is adopted, the distinction between soft and hard systems and system failures is neither a natural nor a useful one. Any system, regardless of its attributes and nature, must be analysed in a systematic way and the generic approach should be the same.

Following from that one can conclude that the methodology for system analysis should be the same for all systems but tools for analysis may be different. The classification of systems, based on the attributes of the system, enabling a selection of the appropriate tools for the analysis, would be much more useful.

Through the work on several projects (Lucic, 2003b) the following conclusions related to systems analysis have been drawn.

The systems we are faced with are most of the time not uniform. Modern high reliability systems are often distributed and consequently the performance of their constituents, subsystems, differs in many aspects (environment, speed, timing) at different places throughout the system.

Nevertheless, the system must be comprehensively defined to facilitate identification of all the hazards.

In generic terms, any system is fully defined by its:

1. Environment;
2. Constituents (different authors use different name for the constituents, objects, parts, etc);
3. Topology of the internal and external interfaces and
4. State of the system.

Environment is defined as the surrounding within which the system works, including people, weather, climate conditions, traffic density, etc. The system can be “self contained” i.e. there can be no interactions between the system and its environment or the system can be “embedded”, i.e. the system receives inputs from the environment and is passing outputs into the environment to fulfil its function. The “embedded” systems can also receive the behaviour rules and disturbances from the environment and can pass the disturbances into the environment.

Constituents or objects are the parts which make up the system, its hardware, software and people. Objects are defined by their attributes which are identifiable and their possible measurable characteristics (Topintzi, 2001).

Objects can be described as the “atomic transformation machines” that transform inputs into outputs in accordance to some transform function. The transform function can be “self contained” i.e. the control mechanism of the transform function can be entirely internal to the object, or it can be “externally controlled”, i.e. the measurement of the output can be passed out of the object and the corresponding control can be fed in the object.

The structure and organisation of connections, interfaces, between the constituents themselves and the constituents and the environment is referred to as the topology of the

internal and external interfaces. The states of the objects and the nature of interconnections (interfaces) and their organisation defines the structure of the system (Topintzi, 2001).

Constituents may change the way they transform inputs into outputs, they can be in different states or the network of interconnections may change its structure, nature or organisation, hence changing the properties and the state of the system. At any moment in time the system may be operating in different states.

It is not unusual that states are grouped into as operational modes. For example, some constituents may be operating in the degraded mode of operation whilst some parts of the system could still operate in the normal mode of operation. In the case of large distributed systems some constituents of the system may operate in different states of operation as well. For example some constituents of the system may be in a preparatory, boot-up stage of operation whilst some of the constituents may be already in full operation.

Formalisation of the notion of a system is offered in (Karcianas, 2003) identifying following definitions in relation to systems' concepts:

Definition 1: A system is an interconnection, organisation of its constituents, objects that is embedded in a given environment.

SYSTEM $\Leftrightarrow$ OBJECTS + TOPOLOGY OF RELATIONS + ENVIRONMENT

Definition 2: An object is a general unit (abstract, or physical) defined in terms of its attributes and the possible relations between them.

Definition 3: For a given object, we define its environment as the set of objects, signals, events, structures, and conditions, which are considered topologically external to the object, and are linked to the object in terms of relations with its structure, attributes through interfaces with the object.

Definition 4: An attribute for an object is an identifiable and possibly measurable characteristic of the object.

Interfaces of the system, inputs and outputs of the system or a system constituent can be generalised in three categories, each of which can be either transferred to other system constituents or be an output of the system:

1. Energy in this case is assumed to be raw energy, motion, heat, electric power, chemical energy;
2. The second category of input or output is defined as information, for example about a state of the nearby system constituent, measured speed or temperature, confirmation status, etc.;
3. Finally the third category of input or output is an action. Action is defined as an act of the system or constituent or environment, on a system, constituent or environment, resulting in a change of a status of the action recipient.

Generalised, any system or a system constituent could be presented by the following diagram:

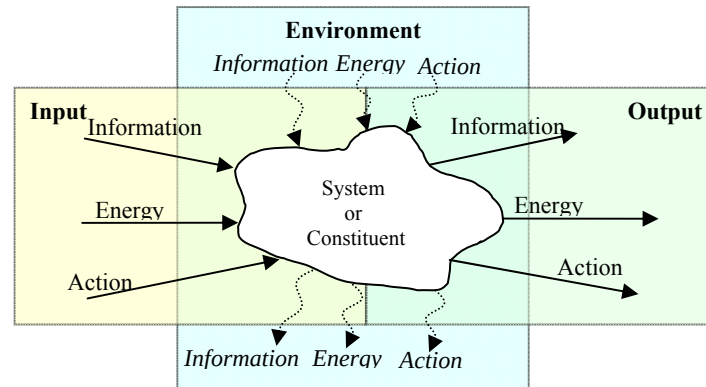


Figure 3-2: Generalised presentation of the system

Combination of the constituents defines the topology of the system, whilst the influence of the environment on the system can be presented as a special case of input/output.

Combination of the constituents' attributes with the environment attributes defines all of the emerging properties of the system.

3.4 Systems Thinking and Reasoning

An essential part of any problem solving, system analysis and decision making process, is *reasoning*. Reasoning is a process of deducing information about a non-perceptible feature of the problem or non-measurable property of the system, based on the available, measured or observed, information about the problem or parts of the system (Bhatnagar and Kanal, 1991).

In a general form reasoning activity can be structured as follows:

- 1 Given/Known:

- 1.1 Information/Knowledge about the observable characteristics of a system/ problem;
 - 1.2 Information/Knowledge about the environment/domain to which the system/ problem belongs.
- 2 Need to determine:
 - 2.1 Some information about some unobserved/unobservable characteristics of a system/ problem.

Three concepts are defined in relation to any reasoning:

1. Innate ideas refer to principles or theoretical truths about the nature in which the reasoner believes;
2. The inputs are the experimental observations made by the observer; and
3. The fact net is an interconnection of inputs and innate ideas constructed by means of a given set of relations and operators, it is a network of contingent truths.

The Inquiry System (Portland and Turoff, 2002) is defined as a process followed by someone, a group of people or something with an aim to create a network of facts in order to establish the overall truth. The enquirer starts off the Inquiry System with an *assumed* “raw data set”. The data set is at the beginning considered to describe a characteristic property of the “real world”.

This is because to begin describing the “world” and enquirer’s “knowledge” of “it”, the enquirer has to invoke a particular “conceptualisation” or Inquiring System characterisation of “it”.

Next, the Inquiry System applies some transformation to the “raw data” creating an input to the model. The model or the fact net, which is any sort of a structured process, is in fact a set of rules. Rules may be either in the form of an algorithm or a set of heuristic principles.

The model transforms the “input data” into “output information”. Finally the output information may be processed again to put it in the right form so that a decision-maker can use it.

Inquiry Systems are differentiated from one another with respect to the priority given to the various steps of the process or the degree of interdependence assigned to the various steps of the process by each Inquiry Systems.

There are 5 core Inquiry Systems (Linstone and Turoff , 2002):

1. Leibnizian Inquiry System: assumes the existence of an a priori model of the system (the innate ideas or the theory describing the system), and attempts to arrange the inputs as to suit the a priori model;
2. Kantian Inquiry System: to begin with, this Inquiry System contains a set of independent models built around an independent set of innate ideas and potentially axioms, primitives and rules of inference. The Inquiry System selects a model from the collection and builds a Leibnizian fact net using this model as a base. Using a preset criterion the Inquiry System determines the extent to which the fact net is satisfactory. The model that produces the most satisfactory fact net is the solution to enquiry;
3. Hegelian Inquiry System: is a dialectic Inquiry System. It seeks to acquire the ability to see the same inputs from different points of view. The concept is based on the premise that for each thesis there is an antithesis. The antithesis does not have to be a logical negation of the thesis, it may be simply a thesis supporting a different view of the same input to the system or different understanding of the effect of the same input on the system. To begin with this Inquiry System contains a set of independent models built around an independent set of innate ideas and potentially axioms, primitives and rules of inference. The Inquiry System ascertains a model that demonstrates that there is a way to look at reality which fits the selected model. Following that the Inquiry System ascertains the model that supports the antithesis. The final step of the Hegelian Inquiry System is development of a “synthesis” model of the system, or a model that would examine and resolve the conflicts between the thesis and antithesis models;
4. Lockean Inquiry System (Portland and Turoff, 2002) postulates that the truth content of a system being observed is associated *entirely* with its empirical content. A model of a system is an *empirical model* and the truth of the model is measured in terms of its ability to reduce every complex proposition to its simple empirical referents. The validity of each of the referents is assured by means of the widespread, freely obtained *agreement* between different observers. The accuracy of the model is not dependant on the prior assumption of any theory. The data input is not only prior to the formal model or theory sector but it is separate from it as well. The whole of the Lockean Inquiry System is built up from the data input;

5. Singerian Inquiry Systems: the truth content of a system is relative to the overall goals and objectives of the inquiry. It is said that for these Inquiry Systems the truth is pragmatic. A corresponding fact net or the model of the observed system is explicitly goal-oriented. The precision of the model is measured with respect to its ability to define systems objectives, to propose alternate means for securing these objectives, and to specify new goals (discovered only as a result of the inquiry) that remain to be accomplished by some future inquiry. It is referred to as a teleological Inquiry System.

Most of the time the information that is available to the Inquiry System is uncertain as described further, later in this report. In these situations the analyst (Bhatnagar and Kanal, 1991), (Portland and Turoff, 2002) is faced with following options:

1. A Leibnizian approximate Inquiry System is concerned with determining the uncertainty associated with the proposed solution model given the uncertainties related to inputs and the innate ideas or determining the imprecise version of the solution model such that the solution can be proven to be correct (“true”) given the uncertainties related to the inputs and the innate ideas;
2. A Kantian approximate Inquiry System would attempt to determine the ordered list of several models that provide the best explanation of the inputs. The imprecision associated with the solution model could be used as a criterion to select a preferred solution model;
3. A Hegelian approximate Inquiry System would attempt to determine the pairs of models in support of thesis and antithesis. The precision of information embedded in the models would be then used as a criterion for selection of a solution model.
4. A Lockean Inquiry Systems are the personification of *experimental, consensual* systems. Lockean Inquiry Systems create an empirical, inductive representation of a problem domain, starting from a set of elementary empirical judgments (“raw data,” observations, sensations). From these an ever expanding, increasingly more general fact net of the real propositions is created.
5. Singerian inquiry is a nonterminating Inquiry System. Singerian inquirers never give final answers to any question although at any point they seek to give a highly refined and specific response. No single aspect of the system has any fundamental priority over any of the other aspects. The observed system is treated as an inseparable whole. It takes holistic thinking to the extreme and aims to constantly include new variables and additional constituents to broaden the base of concern.

It is an explicit postulate of Singerian inquiry that the systems designer is a fundamental part of the system, the system designer must be explicitly considered in the systems representation as one of the system constituents. The designer's psychology and sociology are inseparable from the system's physical representation. Singerian inquirers are the personification of interdisciplinary systems. In a way the Singerian Inquiry Systems are meta- Inquiry Systems, they constitute a theory about all the other Inquiry Systems (Leibnizian, Lockean, Kantian, Hegelian). Singerian Inquiry Systems include all the previous Inquiry System as submodels in their design.

Different models of enquiry are better suited for different problems.

The Leibnizian Inquiry System is an obvious choice in situations where it is known that a good model or theory is available.

If we believe that the truth is equally dependant on the model and the data, then the most appropriate Inquiry System is the Kantian model.

The Hegelian Inquiry System is most appropriate for ill-structured problems where the true is more likely to emerge from a clash between a thesis and antithesis.

The Lockean Inquiry Systems are appropriate for problems where data are prior to the development of formal theory.

The Singerian Inquiry Systems are best suited for complex system analysis problems where completeness of analysis is paramount.

In addition to above described Inquiry Systems, a number of methodologies for structured group analysis have been developed as well. The most common one is known as Delphi.

Delphi is a method for structuring a group communication process in support of an effective technique allowing a group of individuals to deal with a complex problem.

There are two forms of Delphi method. The most common is the paper-and-pencil form, commonly referred to as a "Delphi Exercise." A questionnaire is designed and distributed to a group of experts. The questionnaire is evaluated and the results are distributed to the same group of experts who are given at least one chance to review the original answers. We shall denote this form *conventional Delphi*. The second form of Delphi technique, sometimes called a "Delphi Conference", utilises a computer programmed to carry out the analysis of the group results. This eliminates the delay

caused in analysing the results turning the process into a real-time communications system.

Delphi process can be broken into 4 phases. The first phase is exploration of the subject under discussion. During this phase each participant freely contributes information pertinent to the analysed subject or system. The second phase strives to identify any disagreements between the participants. The third phase is aimed at resolving the differences and evaluating them. Finally when all previously gathered information is analysed and the results are fed back for consideration.

3.5 Models and modelling

Modelling is a process of approximation of the real world, in order to aid representation and understanding of the system and to predict the behaviour of the emerging properties of the system.

Mathematical modelling is a term used to describe the method of approximation of the real world using mathematics (Open University Handbook). A mathematical model is a mathematical relationship linking the variables representing the possible states of the real system.

All models are characterised by their geometric/logical structure and if applicable, the algebraic structure providing the mathematical base of the model.

The two main categories of models are:

1. Descriptive models support understanding of the problem by means of providing structural insight;
2. Decision models support the decision making process. The main requirement on these models is to order the preference of one option over another.

Most of the models are causal models. These models are based on the knowledge of causality relationships which underpins the determination of relating events and the causal structure for a scenario.

Tversky and Kahneman 1982, (Bhatnagar and Kanai, 1991), state “It is a psychological commonplace that people strive to achieve a coherent interpretation of the events that surround them, and that the organisation of the events by schemes of cause-effect relationships serves to achieve this goal.”

There are two approaches to modelling:

1. Qualitative models describe the real world but do not provide any numerical information in relation to model attributes.
2. Quantitative models, on the other hand approximate the real world using some form of numerical or combined graphical and numerical technique.

The causal structure (Bhatnagar and Kanal, 1991) underlies observed symptoms of every situation. Most of the time the observable knowledge is incomplete and consequently it is difficult if not impossible to uniquely identify the underlying causal model.

In situations like this one may need to develop number of different models and then select the most suitable one.

Quantified risk based modelling is increasingly becoming the method of choice for risk assessment. However risk assessment models are notoriously difficult to validate and verify.

Some scientists believe that it is not possible to verify and validate any model. This argument is based on the fact that natural systems are never closed and consequently models created to represent these systems are never unique. Therefore, according to this school of thought (Saltelli, 2002), models can only be “confirmed” by the demonstration of agreement or non-contradiction between observation and prediction.

Modelling as a process can be split into following steps:

1. The first step of the modelling process is the identification of the problem, who or what is potentially affected by the problem and what are the parties involved in the problem;
2. Prior to commencing modelling it is desirable to formally describe the system to be modelled. This stage of the modelling process is usually referred to as the Conceptual modelling. Conceptual modelling has three distinct phases, elicitation, formalisation (processing) and representation of knowledge. This stage of modelling process provides a structured approach aimed at gaining the understanding of the problem domain and development of the description of the system to be analysed.

Development of the model involves creation of the model to encompass all relevant factors within a logical structure capable of simulating the behaviour of the analysed system. This is an iterative process and involves refinement of the conceptual model and

the model itself. In some cases, if the analysed system is complex, it is necessary to produce a hierarchy of models.

There are two types of complexity that may lead to the development of hierarchical models. If the analysed system is complex in terms of its size, number of elements and topological intricacy it may be prudent to develop a high level model describing the behaviour at the level of subsystems and more detailed models for each of subsystems.

Subsequently these models can be integrated into a single model or all of the models can be treated as separate entities with the high level model being manipulated using the data derived through detailed models simulations. If the analysed system is complex in terms of diverse nature of behaviour or characteristics of system constituents, for which different modelling techniques are required, it may be necessary to use different modelling techniques to model different constituents of the system. Once the analysis is completed, these models can be integrated as well.

After the modeller is satisfied with the model it can be used in support of system analysis and evaluation of different options for design or change to be introduced to the system. Important part of this stage of modelling is Sensitivity Analysis, the exploration of uncertainties in the model and how these can be apportioned to different sources of the uncertainty in the model input.

3.6 Review of existing analysis methodologies

3.6.1 System Description Models

Many different methods are used to represent a system. Broadly these may be categorised in two groups:

1. Static models describing the system constituents and their interactions;
2. Dynamic models describing systems behaviour.

Static models mainly describe the system and its constituents. The most frequent model is the System Decomposition Model. System decomposition models often have a hierarchical structure whereby at the highest level only the large subsystems are presented and then each of the subsystems is broken down into more detailed presentation and so on. These models are essentially directed graphs, where shapes (nodes) present system constituents, and directed arrows (edges) represent their internal and external interfaces.

Often, these models are used to capture/represent more than just the basic information such as:

1. Type of interface (command/information);
2. Type of system/subsystem constituent (hardware/software/human) and
3. Boundaries between system and its environment including interactions between the system and environment.

The example of these models is presented by Figure 3-3 and Figure 3-4 below.

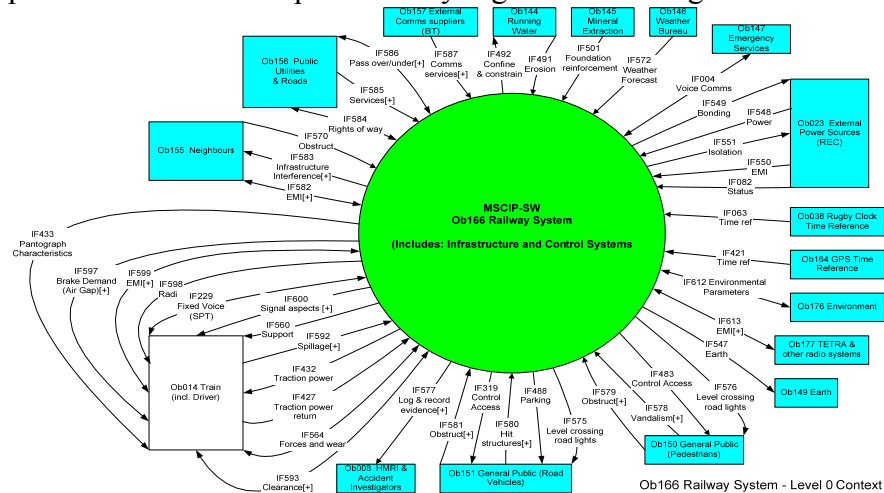


Figure 3-3: An example of the system decomposition model.

This type of the system decomposition models is often referred to as the “Bubble Diagram”, bubbles represent the subsystems and rectangles constituents at lower level of decomposition. Directed lines are interfaces that link up subsystems and constituents into a system.

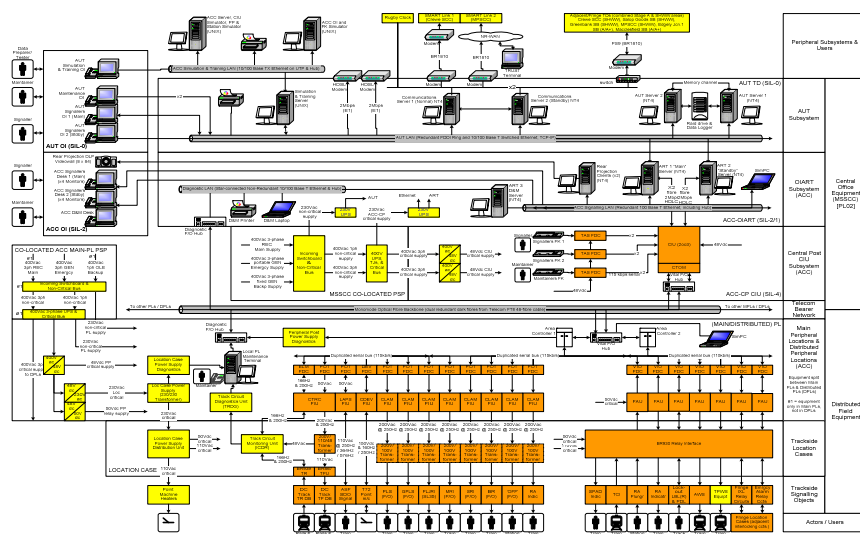


Figure 3-4: An example of the system decomposition model.

A common feature of all decomposition models is that system constituents (constituents or subsystems) are presented by shapes and internal and external interfaces (action, energy or information “carriers”) by directed lines, indicated direction of the exchange.

Of dynamic models the State Transition and Sequence and Collaboration models are seen as the most useful.

The State transition models consist of states (all possible states of the system), triggers (triggers for a system to enter or exit a state) and arrows indicating a direction of a change of a state. An example of the state transition diagram is presented in Figure 3-5 below.

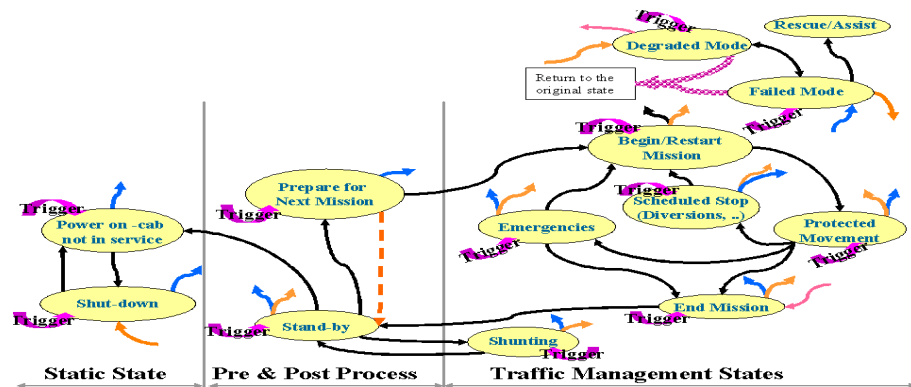


Figure 3-5: State transition diagram of a railway system from a train point of view.

State Transition Models (Pukite and Pukite, 1998) are directed graphs, representing the state space of a system in a given context, the events that cause the transitions and transitions between the states and resulting actions. These models are used to capture knowledge about the system behaviour and can be translated into other models (for example Markov models as discussed later in the report) to support quantified analysis.

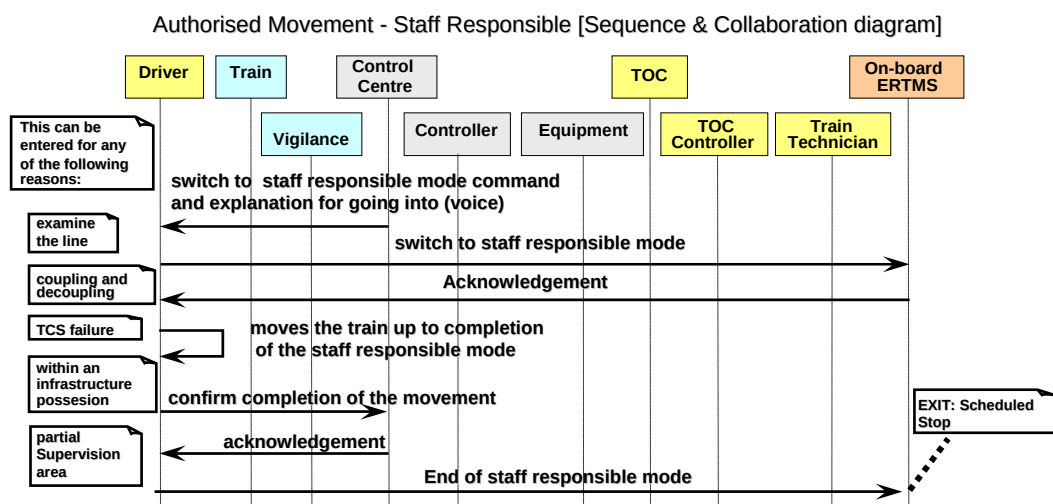


Figure 3-6: An example of sequence and collaboration diagrams

Sequence and collaboration diagrams (models) are interaction models that capture dynamic nature of energy, information or action exchanges between system constituents or a system and the environment. For each state of the state transition model a sequence and collaboration model can be produced to represent the system interactions for each system state.

System constituents are represented by shapes (usually rectangles) from which a vertical line (representing the existence of the relevant shape in time) is drawn downwards to capture the time and directed lines (arrows) representing the exchanges between system constituents. Shapes (usually folded corner rectangles) represent the entry and exit points.

These models are useful in support of system conceptualisation and definition and analysis as they are capable of encapsulating information related temporal and spatial aspects of the system behaviour.

This technique has been used by the author of this report in support of a large scale project aiming to define safety requirements for European Railways Traffic Management System (ERTMS).

3.6.2 System Dynamics

System Dynamics is defined (Topintzi, 2001), (Sterman, 2000) as a rigorous method for qualitative description, exploration and analysis of complex systems in terms of their processes, information, organisational boundaries and strategies; which facilitates quantitative simulation modelling and analysis for the design of system structure and behaviour . It is a quantitative technique for evaluation of the dynamic behaviour of socio-technical systems and their response to the stream of decisions created in response to changing inputs of information.

Systems Dynamics modelling methodology is used to investigate the combined effects of individual changes made at different points in a system. The model-building approach of System Dynamics attempts to include and quantify all factors that influence the behaviour of the observed system or its parts. Two basic symbols are used in System Dynamics modelling:

1. Accumulation of something (information, energy, etc), represented by rectangle;
2. Flow or movement of anything (people, action, etc), represented by directed lines.

Together these basic elements, form cause and effect loops

A vital principle of System Dynamics is to incorporate all information believed to significantly influence behaviour into the model, leaving out unnecessary detail. System Dynamics is also problem-centred, or goal-centred.

Together, accumulations and flows form cause-and-effect loops that model problem development over time and identify the likely consequences of the system.

Systems dynamics methodology was developed by the Massachusetts Institute of Technology professor Jay W. Forrester in 1961.

As a methodology for analysis (and management) of complex feedback systems, it has been used to address practically many different kinds of feedback system. The System Dynamics caters for description of the behaviour over continuous time and identification of a system boundary to include the areas of interest for research and analysis.

It provides a structured format for identifying and depicting feedback system elements, goals, discrepancies, levels, rates and flows of information and controls.

The author of the thesis did not use this methodology in practice for following reasons:

1. System Dynamics modelling as a technique is suitable for high level abstraction. However models required to support systems analysis on railways must be capable of supporting relatively detailed, low level of abstraction;
2. It appears that in cases of more complex System Dynamics models, and in case of railways certainly the system models are very complex, it is practically impossible to calibrate these models.

3.6.3 Risk Matrix (Rapid Ranking)

Frequency-severity risk matrices are often used in support of risk analysis. They are matrices of likelihood and consequence categories. Individual risk values of cells of the matrix are assigned using qualitative analysis. However, risk matrices are only appropriate for prioritisation of risks to be further analysed or acted upon.

The Risk matrices are deficient for following reasons:

1. Subjective and without auditable justification;
2. Coarse, usually leading to overestimation of risk;
3. Based on extrapolated judgmental assessment of frequency of safety consequence arising from a hazard, missing the consequence analysis and therefore not covering the intricacies of all risk mitigation measures nor including the related consequences of other hazards.

3.6.4 Failure Mode and Effects (and Criticality) Analysis

Failure Mode and Effects (and Criticality) Analysis (FMEA/FMECA) are structured methodologies for identification and analysis of effects of latent equipment failure modes on the system performance. This is a bottom-up process starting with the failure of a constituent/subsystem and investigating the effect of this on the system. It should

be conducted by a team of experts with cross-functional knowledge of the analysed system, process or product. The methodology consists of the following steps:

1. Identify the object of the analysis (part, subsystem, step in the process, etc);
2. Identify the function related to the object of analysis;
3. Identify the failures of the object of the analysis;
4. Identify the effects of different failures on the object of analysis and the system which the object is part of;
5. Identify the causes of the failures;
6. Identify and analyse existing controls in place to mitigate the failures;
7. Identify any additional potential controls;
8. Prioritise implementation of corrective actions using a consistent standard;
9. Recommend actions to implement to minimise the risk.

The criticality analysis includes the estimation of probability of occurrence and severity.

3.6.5 Theories of probability

The two probabilistic theories that will be mentioned in this thesis are conditional probability and Bayesian Belief Networks (BBN).

Conditional probability theory was developed a long time ago, but still is one of the most useful tools for analysis of uncertainty. Let us consider two variables A and B with the associated sets of their possible values $(a_1, a_2, a_3, \dots, a_n)$ and $(b_1, b_2, b_3, \dots, b_n)$.

Now if we know the conditional probability of $P(a_i | b_j)$, whenever the event $B=b_n$ is observed, the probability value of unobserved event $A=a_m$ can be calculated.

Bayesian Belief Networks are directed acyclic graphs. The nodes represent uncertain variables and the edges are the causal or influential links between the variables.

Associated with each node is a set of conditional probability values that model the uncertain relationship between the node and its parents.

The theory of BBN combines the Bayesian notion of conditional independence and probability theory. Once a BBN (Fenton, Neil and Forey, 2001) is built, it can be executed using an appropriate propagation algorithm.

This involves calculating the joint probability table for the model (probability of all combined stages for all nodes) by exploiting the BBNs conditional probability structure to reduce the computational space:

$$\begin{array}{c} \text{posterior_failure_rate_} \\ \text{distribution} \\ p(\lambda|e) \end{array} = \frac{\begin{array}{c} \text{likelihood_of_evidence_} \\ \text{given_the_failure} \\ p(e|\lambda) \end{array} \begin{array}{c} \text{prior_belief_about_} \\ \text{the_failure_rate} \\ p(\lambda) \end{array}}{\begin{array}{c} p(e) \\ \text{evidence} \end{array}} \quad \text{Equation 1: BBN}$$

Following diagram is a representation of a BBN.

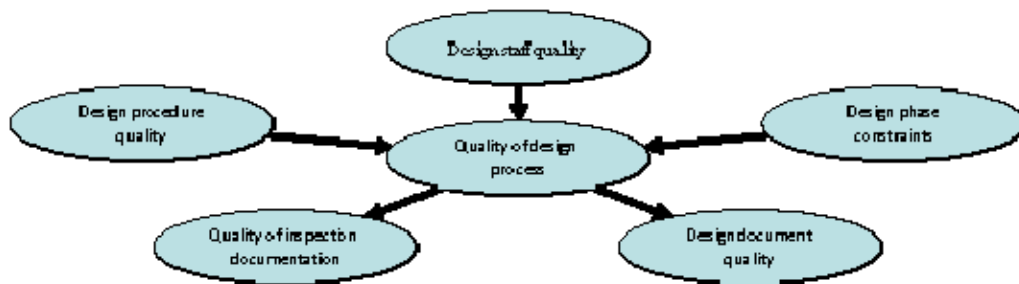


Figure 3-7: BBN representation

Once a BBN has been compiled it can be executed and exhibits the following two key features:

1. The effects of observations entered into one or more nodes can be propagated throughout the net, in any direction, and the marginal distribution of all nodes updated;
2. Only relevant inferences can be made in the BBN. The BBN uses the conditional dependency structure and the current knowledge base to determine which inferences are valid.

3.6.6 Monte Carlo Simulation models

Monte Carlo methods are statistical simulation methods that use sequences of random numbers to perform the simulation. With these methods, a large model of a system is sampled in a number of random parametric configurations, and the resulting data is used to describe the emerging properties of a system as a whole.

As opposed to a conventional numerical solution approach, which would start with the derivation of differential equations describing the mathematical model of the physical system, and then discretising the differential equations to solve a set of algebraic equations for the unknown state of the system, the Monte Carlo methods use random

sampling techniques to arrive at a solution of the physical problem. Sometimes it is necessary to use other algebraic methods to manipulate the outcomes of Monte Carlo simulations.

When using Monte Carlo methods, the real, physical process is simulated directly, and there is no need for derivation of the differential equations to describe the behaviour of the system.

The only prerequisite is that the system or a model of the system can be described by a probability density functions. However, obtaining the accurate probability values and understanding the probability density functions can be difficult.

Sometimes it may be necessary to carry out supplementary experiments or develop additional models in order to obtain sufficient information to input into the Monte Carlo model.

In many applications, it is possible to predict the statistical error (the “variance”) of the result, and consequently it is possible to estimate the number of Monte Carlo trials that are needed to achieve a given error intervals.

3.6.7 Theory of Evidence

In 1976, Shafer (Bhatnagar and Kanal, 1991) developed the theory of evidence.

Probability theory states that if “S” is the universal set of events, then the uncertainty information consists of a probability density function, “p” such that

$$p: S \rightarrow [0, 1] \text{ and } \sum_{s \in S} p(s) = 1 \quad \text{Equation 2: Theory of evidence}$$

In the theory of evidence a mass function is used. The mass function is induced by the available evidence and it assigns parts of finite amount of belief to subset of “S”. Each assignment of a mass to a subset “s” of “S” represents that part of our belief that supports s without being able to allocate this belief among strict subsets of s.

The degree of belief in a subset “A” of “S”, “bel(A)”, is defined as the sum of all masses that support either “A” or any of its strict subsets:

$$bel(A) = \sum_{X \in A, X \neq \emptyset} m(X). \quad \text{Equation 3: Degree of belief}$$

The degree of plausibility of a subset “A” of “S”, “Pl(A)” is defined as

$$Pl(A) = \sum_{X \cap A \neq \emptyset} m(X) \quad \text{Equation 4: Degree of plausibility}$$

or the sum of all the masses that can possibly support “A”. The possibility of a subset “s” supporting “A” means that the mass assigned to “s” can possibly gravitate to that strict subset of “s” which is also a subset of “A”.

3.6.8 Reliability Block Diagrams and Network models

Reliability Block Diagrams (RBD) are used to show a highly abstract (Pukite and Pukite, 1998) view of the system redundancy. The RBDs are simple, well known and easy to evaluate. They use blocks to represent system constituents (Goble, 1998).

The blocks are arranged to correspond to constituents required for successful operation. If there is a path through the block diagram with all the blocks being successful this constitutes the operation being successful.

However, only two states can be represented for each constituent by RBD. This is a serious limitation since more often than not it is necessary to consider more than two states of each system constituent as part of the analysis. Network models are very simple models consisting of nodes and communication links. They are used to represent communication networks with individual links.

3.6.9 Fault Trees - Event Trees

Fault and Event Trees are formalized diagrammatical models that trace paths from a top Hazard (unwanted event) to the basic input events via logic gates and development of a Hazard through to the consequences resulting from success or failure of systems intended to mitigate effects of the initiating event.

A starting point of the Fault-Event Tree (FET) analysis is always the Hazard (Goble, 1998), (Hessami, 1999a), (RSSB, 2007).

These models can be used qualitatively, to capture and represent the scenario that gives a rise to a hazard and subsequently to its consequences, thus supporting options analysis and identification of new potential mitigations.

Moreover these models are used to quantify the frequency/probability of occurrence of a hazard and its consequences, thus potentially supporting impact assessment. An example of the Fault –Event Tree is presented in Figure 3-8 below.

Although the Fault –Event Tree models are used frequently, these modelling technique has some serious limitations:

1. The FET analysis is capable only of presenting a snapshot in time. Therefore if different system configurations exist during different phases of a mission, this technique cannot be readily used;
2. The FET analysis does not include loss analysis therefore it does not support the complete risk assessment as such, but only a part of it;
3. Temporal and spatial aspects of the system behaviour cannot be modelled by this technique;
4. The FET model can only represent one system configuration at the time.

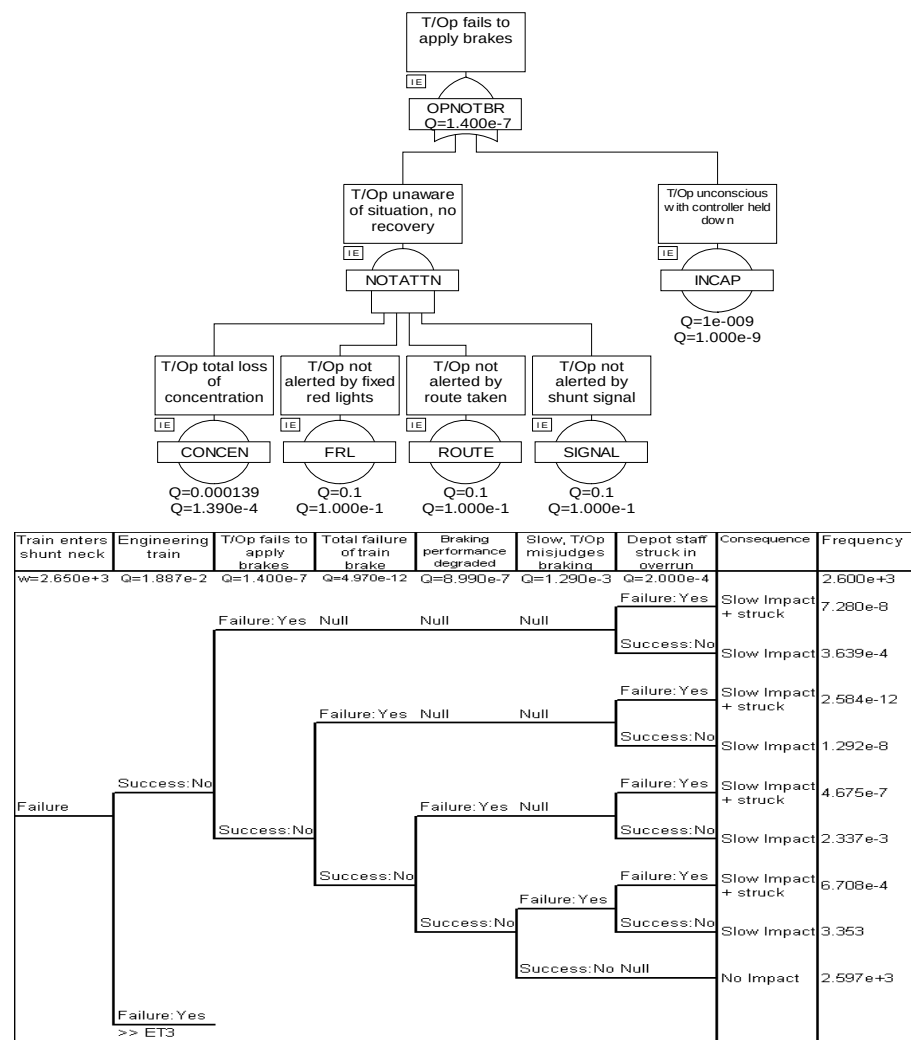


Figure 3-8: An example of Fault and Event Tree

3.6.10 Markov models

Markov models use state transition diagrams as its base. This technique uses only two symbols (Rouvroye, 2001); a circle to represent the successful/failed system constituents and a directed arc to represent possible constituent failure and repair.

The Markov models consider system states and possible transitions between them (Pukite and Pukite, 1998). The basic assumption in a Markov model is that the system has no memory and that consequently, transitional probabilities are defined purely by the present state and not its history.

Probabilities of operation are calculated in each state as a function of time taking into consideration the failure rates and repair rates.

3.6.11 Petri Nets

Petri nets are a graphical and mathematical modelling tool (Pukite and Pukite, 1998) and (Topintzi, 2001).

Basic objects of Petri nets are places (represented by circles), transitions (represented by bars), and arcs that connect them. Input arcs enter transitions from places and output arcs start leave transitions and enter places. More symbols can be used.

Places represent discrete states whilst transitions are active constituents. They model activities which can occur (the transition *fires*), thus changing the state of the system (the marking of the Petri net).

Transitions are only allowed to fire if they are enabled, which means that all the preconditions for the activity must be fulfilled (there are enough tokens available in the input places).

When the transition fires, it removes tokens from its input places and adds some at all of its output places.

As a graphical tool, Petri nets capture and represent the dynamic and concurrent properties of system.

It is possible to set up state equations, algebraic equations, and other mathematical models governing the behaviour of systems.

Petri nets can model a variety of situations and are easy to understand.

However, the underlying model is difficult to solve. A larger model may become very complex and a solution may require use of Monte Carlo tools.

3.6.12 Theory of Fuzzy Sets

Fuzzy logic simulates human decision making process, with ability to generate precise solutions from certain or approximate information. While most of the other conceptions require an accurate mathematical model to simulate real-world behaviours, fuzzy logic is capable of using real-world human logic and even language.

Using fuzzy logic reduces the time required to interview and interpret a domain expert's knowledge of risk sources and consequences, while still capturing any uncertainty in the expert's opinion.

Fuzzy logic is an alternative way to simulate uncertainty. Fuzzy number sets have a range, the wider the range the more uncertainty introduced in the system. Fuzzy numbers have a degree of membership between zero and one associated with each point in the range.

The degree of membership is not a probability density function. The mean of the degree of membership curve can be found mathematically as the centroid of an area defined by the curve. The degree of membership curve does not need to integrate to 1, and integration of the curve does not produce a cumulative density function. There is no probability associated with the extremes of the range or any point within the range. Monte Carlo simulations are not needed for fuzzy numbers.

Fuzzy logic is a superset of Boolean logic, which has been expanded to accommodate the concept of the degree of truth-values, between the "absolutely true" and "absolutely false".

The concept allows for mathematical modelling of the modes of approximate reasoning. The essential characteristics of fuzzy logic are:

1. Exact reasoning is perceived as a limiting case of approximate reasoning;
Everything is a matter of degree;
2. Any logical system can be fuzzified;
3. Knowledge is interpreted as a collection of elastic or, equivalently, fuzzy constraints on a collection of variables;
4. Inference is viewed as a process of propagation of elastic constraints.

All the decisions humans make are based on rules, if-then statements. Rules relate ideas and link one event to another, establishing cause-consequence relationships.

Fuzzy logic mimics these decision making processes; a decision and the means of choosing that decision are replaced by fuzzy sets and the rules are replaced by fuzzy rules. Fuzzy rules operate using a series of if-then statements.

Each fuzzy rule defines a “patch”, a segment, of the decision making process curve. A finite number of patches can cover a complete curve, defining the complete “decision” curve. If patches are large, then the rules are loose, if patches are small then the rules are refined.

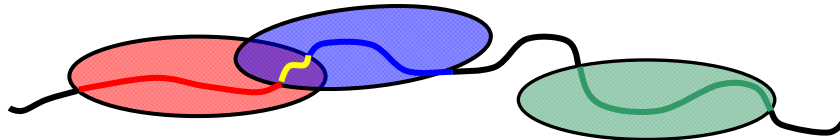


Figure 3-9: Fuzzy Patches

Fuzzy processors use expert knowledge expressed as a set of rules instead of, for example, differential equations to describe the system. A set of rules can be defined based on the expert knowledge using linguistic variables, which are described by fuzzy set.

A linguistic variable is a quintuple $(X, T(X), U, G, M)$, where “X” is the name of variable, $T(X)$ is the term set, set of names of linguistic values of “X”, “U” is the universe of discourse, “G” is the grammar to generate the names and “M” is a set of semantic rules for associating each “X” with its meaning.

Three steps are taken to create a fuzzy process:

1. Fuzzification (Transformation of measurements/crisp values into fuzzy values);
2. Rule evaluation (Application of fuzzy rules, also known as inference);
3. Defuzzification (Obtaining crisp values or actual results).

The employment of Fuzzy Processors is recommended for very complex processes, when there is no a simple mathematical model, for highly nonlinear processes and if the processing of linguistically formulated knowledge is to be performed.

If we define a process surface as a hyper-plane derived from a multiple set of process inputs/output relationships it will be possible to relate inputs to outputs, and tune the processor by altering the rulebase and comparing the effect on the process surface. Each point on the plane has its coordinate, $[x \ y \ z]$, defining the position within the envelope relating inputs, $[x \ y]$ to output $[z]$. This means that the fuzzy processor can be tuned by shaping the process surface, rather than by adjusting numerical gains.

Furthermore it allows for complex, multiple process goals nonlinear systems to be defined by relatively simple distortion of the process surface shape. Each rule in the rulebase defines a separate processor goal. Changes to individual rules do not have a global effect on the process surface thus the processor action can be locally tuned to suit specific need.

Overlaps of the fuzzy sets, allowing a smooth transition between rules, define an area of the input range where multiple input sets can be activated. This area is known as the Area of Influence. Increase of the overlap level, between the fuzzy sets, increases the proportion of the process surface contained within the Area of Influence.

Since the de-fuzzified crisp value of the process output is located within the Area of Influence, increase of the proportion of the process surface contained within the Area of Influence, smoothes the processor action. In order to smooth the process action, but keep the ability to distinguish between the regions of the process surface at the same time, an overlap of the fuzzy sets should not extend over more than 50%.

In order to compromise between the smoothness of process and resolution of surface, it is possible to use more advanced sets of shapes as membership functions, such as bell shaped membership functions instead of simple triangular shaped ones, to describe the fuzzy set.

3.6.13 Weighted Factors Analysis

Weighted Factors Analysis (WeFA) methodology is a creative knowledge capture, representation and evaluation methodology (Lucic, 2004a), (Hessami, 1999a), (Hessami, 1999b) and (Hessami and Hunter, 2002). It enables the knowledge about the given problem to be captured and represented at a high and strategic level. WeFA methodology supports a holistic approach to problem solving.

In contrast with a risk based perspective focusing on hazards alone, WeFA analysis also highlights the opportunities which require effort at enhancement and optimisation alongside reduction in risks. The knowledge elicitation process is group based, exploiting the diversity of expertise and perspectives. This, first, stage of the analysis is focused around a task identification of an AIM. The AIM is common goal/objective of the undertaking or a system being analysed.

Once an AIM is defined and agreed (for example the AIM may be “Enhancements of the system performance”) the group is encouraged to identify the highest level DRIVERS and INHIBITORS which are likely to influence the AIM. The DRIVERS are

defined as factors that contribute to the AIM and the INHIBITORS as factors that are detrimental to the AIM.

An example is presented by Figure 3-10 and Figure 3-11 below. Let us assume that the study seeks to analyse factors influencing safe driving. So, the agreed aim is “Safe Driving”. Furthermore, let us assume that the workshop participants concluded that clarity of rules and procedures and good, comprehensive training enhance the ability of the driver to drive safely. These two will be the DRIVERS. In the same fashion, let us assume that the workshop participants concluded that bad weather conditions could hamper driver’s attempts to drive safely. This is the INHIBITOR in the WeFA terminology.

The elicitation process should continue for each DRIVER and INHIBITOR depending on the need to understand its properties. The elicitation is terminated within the branch when the group feels sufficient clarity has emerged and further decomposition is not likely to add value. Figure 3-11 below, illustrates this approach.

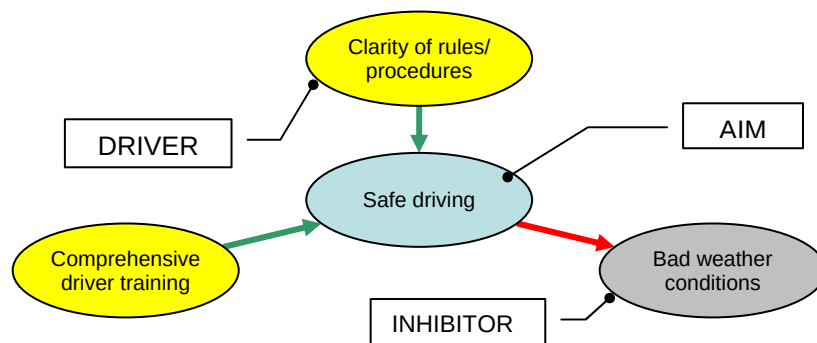


Figure 3-10: WeFA example

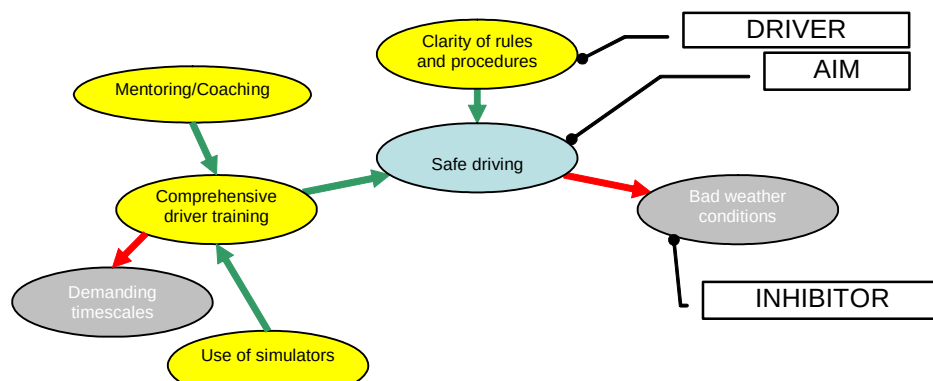


Figure 3-11: WeFA example (expanded)

WeFA underpins following principles:

1. Definition and group argument on the focus of the analysis;
2. Consideration of inherent polar opposites as influencing factors;

3. Hierarchical and successive decomposition;
4. Consideration and inclusion of hard and soft factors into analysis;
5. Simple graphical representation of knowledge;
6. Weighting of factors according to their degree of influence;
7. Explicit representation of dependency between factors;
8. Potential for quantification and treatment of uncertainty;
9. Problem resolution through options identification and evaluation.

the author of this paper used the WeFA methodology in support of a data elicitation for a strategic railway project and it was observed that the WeFA methodology is especially beneficial when used in support of high level, strategic knowledge elicitation (Lucic, 2001).

Although several different technologies have been tried (BBN, Fuzzy) at the moment the general mathematical theory for quantified WeFA analysis is not available.

3.6.14 Advanced Cause – Consequence models

Once the significant hazards within the scope of a product, process or undertaking are identified and recorded, it is desirable and constructive to understand their causality.

This may help in eliminating the hazardous condition altogether or to take actions to reduce its likelihood or frequency. The process is referred to as Causal Analysis. The Modelling methodology used in support of Causal Analysis is commonly known as Fault Tree Methodology.

Irrespective of the extent of preventative measures taken, hazards do occur. It is also desirable to develop an understanding as to how a given hazard is likely to escalate in the real world once it has occurred and what range of incidents and accidents are likely to arise from a hazard.

The idea being that even in occurrence of a hazard, a range of measures may be available to detect, control and avoid accidents or minimise losses associate with such accidents. This process is referred to as Consequence Analysis. Consequence analysis involves establishing the intermediate conditions and final consequences that may arise from a hazard.

It involves bottom-up assessment of each hazard and is focused on the post hazard horizon. The sequence of intermediate conditions identified is termed “the hazard

development scenario”. Defences against potential escalation (the defence may be equipment, procedure or circumstance) are referred to as ‘Barriers’.

The Consequences of a hazard are categorised into three broad categories, Safety, Commercial and Environmental. An example of basic Cause- Consequence risk model structure is given in Figure 3-12.

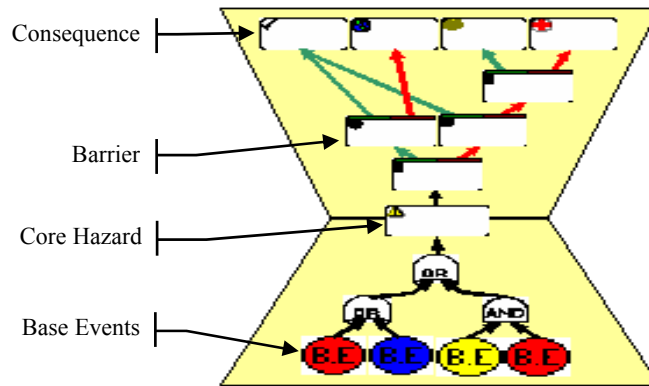


Figure 3-12: Basic structure of the Cause-Consequence Model

The following are objects that are defined within the framework of the advanced cause consequence model:

1. **Base Events** represent different failure modes and events that may trigger the hazard and are related to failures of system constituents. Base events are numerically expressed as failure rates or probabilities.
2. **Logical gates** “AND” and “OR” are used to mimic possible logical combinations of different failures and therefore describe the hazard evolution scenario. Together with base events they make up a “fault tree”.
3. **Hazard or Critical Event** whose probability or frequency of occurrence is calculated by the fault tree.
4. **Barriers** are defences against a hazard. Once a hazards is already “alive” usually there are still some defences, prevention measures which avert the hazard from becoming a consequence. Barriers are defined by the probability of success of the barrier working and therefore preventing the consequence. Therefore barriers have one input, the probability of a hazard occurring, and two outputs, the probability of the barrier working (success) and that of it not working (failure) There are three different types of barriers:
 - a. **Physical Barrier**; equipment based protection measure, for example fire alarm;
 - b. **Procedural Barrier**: procedure based protection for example evacuation

procedure;

- c. Circumstantial Barrier: if consequence is avoided by pure luck. It is beneficial to record these, as it may be possible to turn them, in future, into a physical or procedural barrier and therefore mitigate against the hazard better.
5. **Consequences** are defined as the final outcomes of the hazardous scenario, for example a collision between two trains. The Cause Consequence model calculates the probability or frequency of occurrence of a consequence. To evaluate the risk of a consequence it is necessary to estimate a potential loss associated with each of the consequence. The estimation is not part of cause consequence modelling tool. Consequences are grouped into 4 categories as follows:
- a. Predominantly **Safety** Related Consequence: If predominant loss associated with the consequence is safety related then the consequence is classified as a safety consequence;
 - b. Predominantly **Commercial** Consequence: If predominant loss associated with the consequence is commercial (damage to property, loss of service, etc.) then the consequence is classified as a commercial consequence;
 - c. Predominantly **Environmental** Consequence: If predominant loss associated with the consequence is environmental (damage to nature, release of contaminated materials, etc.) then the consequence is classified as an environmental consequence;
 - d. **Broadly Safe** Consequence: if a hazard occurs but due to Barriers working does not give a rise to a safety, commercial or environmental consequence, in other words if accident is avoided, then this outcome of the hazard development scenario is defined as a Broadly Safe consequence;
6. Internal to model **connectors**, “OUT” and “IN”: due to the complexity of some of the cause consequence models, the modelling technique allows for models to spread across several pages, “work sheets” and for outputs of model elements to be transferred across different “work sheets”. This is realised through use of “OUT” and “IN” symbols. This is purely linking functionality and does not transform the transferred probability or frequency in any way.

Standard Fault Tree analysis rules apply, including a need to ensure that Base Events are independent from each others. It is possible that the same base event may need to

several different consequences and hence appear in several places in the same model. In such cases it must be assured that the base events and relevant data are described and justified within the specific context each time. This can be achieved by means of use of logical gates to combine these Base Events with other ones to capture the specific context.

The Advance Cause Consequence Modelling technique has been further developed into parametric modelling technique and used on several railway projects. The most recent application of the technique is described in the following chapter of this thesis.

3.7 Chapter Conclusions

In this chapter the author presented the findings of the literature research the author carried out. Two specific areas of interest were subject of the research. Firstly system theory applicable to safety engineering, the notion of a system, formal definition of the system as a concept, the modelling process and the reasoning process were investigated and are summarised here. The knowledge gained from this activity has been used as an essential building block in the later development. Following from that, a review of the existing analysis tools and methodologies was carried out and findings from that research are summarised here as well. A more detailed critique of these is provided in chapter 5 of the thesis.

The main criticism of the existing methodologies is that they do not make a holistic, integrated and heterogeneous framework.

However, each of the methodologies described in this section is useful on its own right, and should be used in support of analysis of specific problem area.

Figure 3-13 below provides an overview of all the methodologies reviewed here and their applicability on the problem domain.

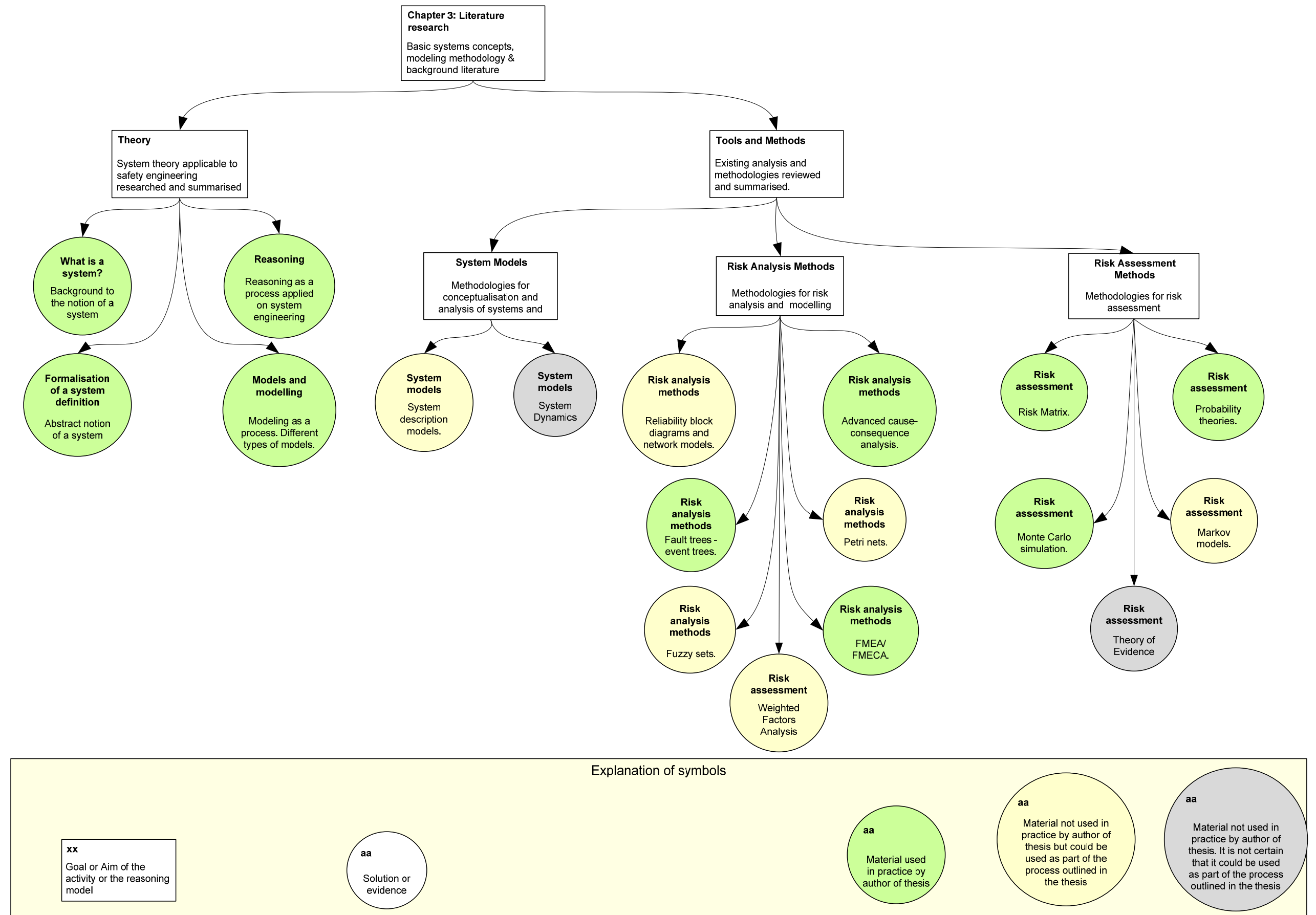


Figure 3-14: Overview of analysed methodologies and their applicability on the problem domain.

CHAPTER 4: The Application Area & Initial Development

4.1 Chapter introduction

As already discussed in the previous section the existing techniques for analysis and assessment of safety risk as an emerging property of the System, do not amount to an integrated methodology for analysis and assessment of complex systems.

Some of the techniques (detailed earlier) the author used in practise, to support delivery of four different projects.

However, it was necessary to develop these techniques further, and in some cases develop new ones, and then integrate them into a coherent, consistent methodology.

Although these four projects provided a drive for further development and a novel approach, due to the limited scopes of the projects at that stage it was not necessary to develop a holistic integrated methodology the Engineering Safety and Assurance Process (ESAP), mentioned earlier in the thesis, as an integrated framework. The Victoria Line Upgrade Programme (detailed later in the thesis) which was at an early stage in its lifecycle (sufficiently early in the project, at design stage) provided a drive/need for and justified the evolution of the processes and the methodology, using the experience and knowledge gathered through work on the four projects depicted in this section, into ESAP.

As part of the research, these projects have been used to test some of the novel concepts and approaches.

The following is the description of the practice and the processes followed. Novel applications of existing methodologies and development of novel methodologies by the author are indicated appropriately.

The structure of this chapter is outlined by Figure 4-1 below.

For each of the projects, the author outlined the purpose and scope of the project and presented the work and research carried out, development of new techniques and results of the work.

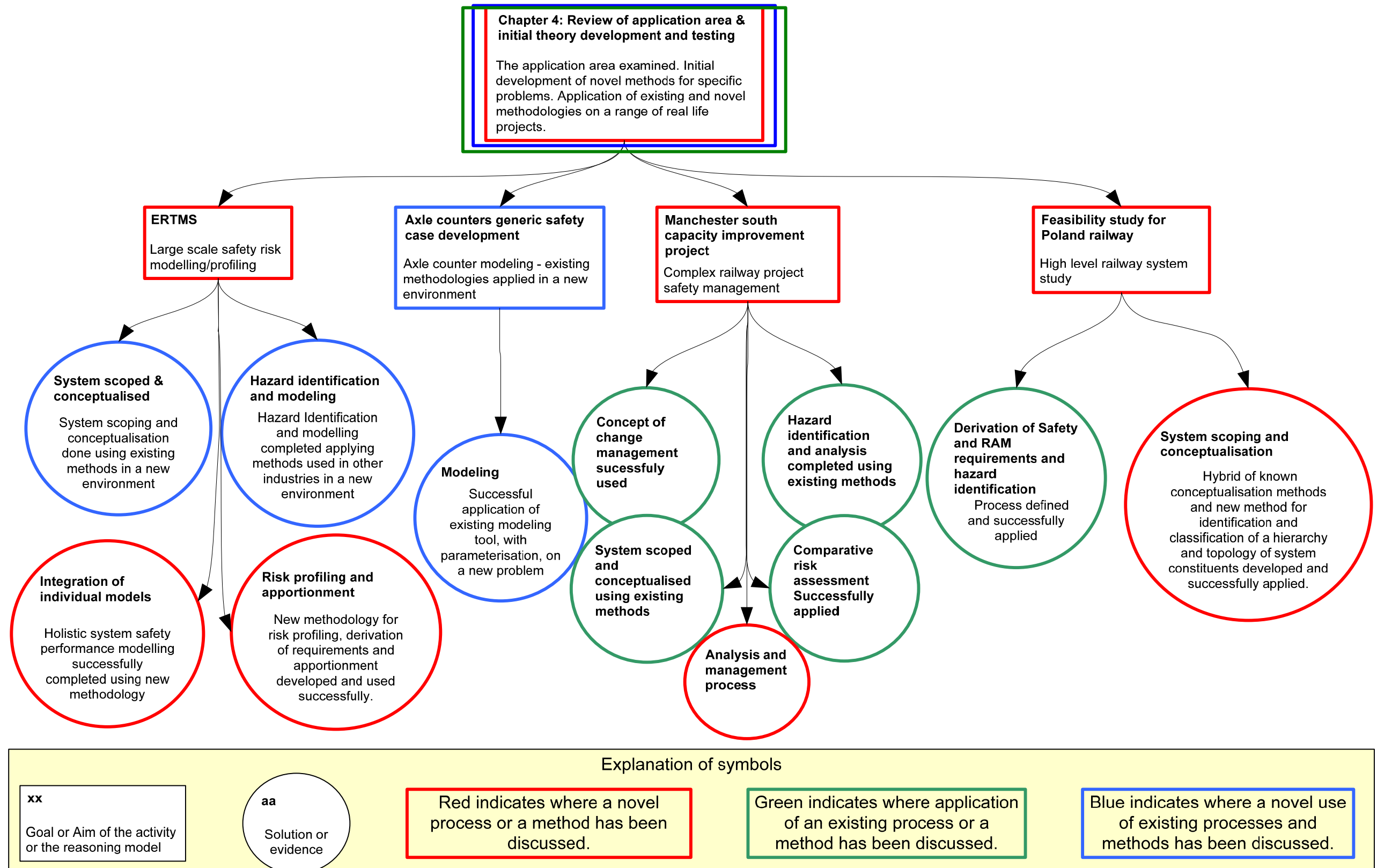


Figure 4-1: Outline structure and the argument presented in Chapter 4

4.2 First Project: Large Scale Safety Risk Modelling – ERTMS

The modelling technique used on the project is novel. The technique and the tools supporting it were developed by the Risk Analysis Unit team of Railtrack Plc. The author was involved in the development of the process and the tools as a member of the team and has developed the algorithms and specification for extension of a tool in support of modelling work as outlined later.

4.2.1 Purpose and Scope of the Project

The purpose of the project was to define and quantify the safety requirements for European Railways Traffic Management System (ERTMS). The European Commission for Transport is managing the project, the biggest pan European engineering undertaking ever in terms of finances involved, geographical spread, required workforce and the complexity of technology involved.

The aim is to connect all European countries with a fully compatible high speed rail network (500 km/hour). Later phases of the project are envisaged to include other former eastern European countries, the Balkans, Greece, Russia and Asian countries.

Standardised safety requirements and safety targets are necessary to achieve full compatibility between trains, railroads (track, signalling, power supply, telecommunications, etc.) and operating rules. A number of novel techniques and extensions of the existing techniques and tools have been used to enable safety risk modelling as follows:

1. Use of state transition and sequence and collaboration models in support of Hazard Identification;
2. Creation of a reference, virtual, railway system used to derive a common data set to enable development of the unified risk model;
3. Extension of existing tools and techniques in support of model integration of individual models into an integrated model, risk profiling and apportionment (Advanced Cause Consequence Modelling has been developed further into the Parametric Advanced Cause Consequence Modelling technique supported by a tool “Integrated Safety Assurance Environment (ISAE)”).

These developments are depicted in following sections.

4.2.2 Problem Description and Conceptualisation

The analysed system is not a uniform system; it is different in many aspects at different places throughout Europe. At the time of the project, three different technical solutions, each with several variants, were planned, to suit diverse needs of national

railways as well as varied financial potential of EU member states. Nevertheless, it was necessary to define the system to facilitate identification of the hazards resulting in a common, universal set of safety targets.

The following is a list of the problems the project has to resolve:

1. No detailed specification;
2. No single system solution;
3. No generic description of a system;
4. Different operational rules in different countries;
5. Different operational environments;
6. Different safety cultures and legal regimes throughout the EU;
7. No uniform data collection system;
8. Different stake-holders;
9. Different activities, tools and techniques;
10. Different degrees and measures of control;
11. Vastly different time-scales & costs;
12. Vastly different risk profiles;
13. Different people and competencies;
14. Different needs (freight versus passenger services, etc.);
15. Different levels of technological development and density of existing infrastructure.

However, initial analysis showed that the system is sufficiently known in generic terms that can be broken down into elements that broadly fit into one of three categories:

1. Environment;
2. Constituents;
3. Operational modes.

Environment is defined as the environment within which the system works, including people, weather, climate conditions, traffic density, etc. Constituents are constituents of the system, its hardware and software and people. Different operational modes are in fact dictated by different technological and procedural solutions to the same problem namely:

- Level 1 operational mode or the railway system as it is now, but operated in accordance with new synchronised operational rules;
- Level 2 operational mode or ‘in cab’ signalling systems where information to the train is transmitted via short distance transmission antennas positioned between rails at carefully chosen places so to mimic the functions of the conventional signal;
- Level 3 operational mode or ‘in cab’ signalling where information to the train is transmitted via radio signal securing continuous and almost instantaneous information update.

Within any operational mode described above a number of operational states, generic situations, was identified, in such a way that, one could say that at any moment in time a train has to be in one and only one state or situation.

4.2.3 System representation and scoping

In support of the system representation and scoping, existing modelling techniques, “State Transition” and “Sequence and Collaboration” modelling were used in a novel way. A high level generic system description has been developed and used as the starting point of analysis, using the state transition model. The focal point of this representation is a train (Figure 3-5, earlier in the report). This, high level description, referred to as “ERTMS State Transition Diagram”, depicts all the possible transitions between different states of a train within the ERTMS operational environment.

Three main classes of system behaviour have been identified:

1. Static States: The train does not move, none of the vital train management functions are engaged and the train is either shutting down or powering on;
2. Pre & Post Process: Preparation for the journey, arming of the computer or resetting the computer data and waiting for change towards “preparation for next mission” ;
3. Traffic Management States: The actual journey including all possible states of a normal journey as well as emergencies and degraded operations.

In total 13 states have been identified:

- Shut Down;
- Power On-Cab Not in Service;
- Stand-By;
- Prepare For Next Mission;
- Protected Movement;
- Begin/Restart Mission;
- Scheduled Stop;
- Rescue / Assist
- Shunting;
- Emergencies;
- Degraded Mode;
- Failed Mode;
- End Mission.

For each identified state a so called pseudo-Spec has been developed, depicting the state itself and transitions from one state to another including the description of the transition trigger.

Subsequently, the “ERTMS State Transition Diagram” has been further analysed and each of the individual states has been described in detail using the “Sequence and Collaboration” analysis (Figure 4-2).

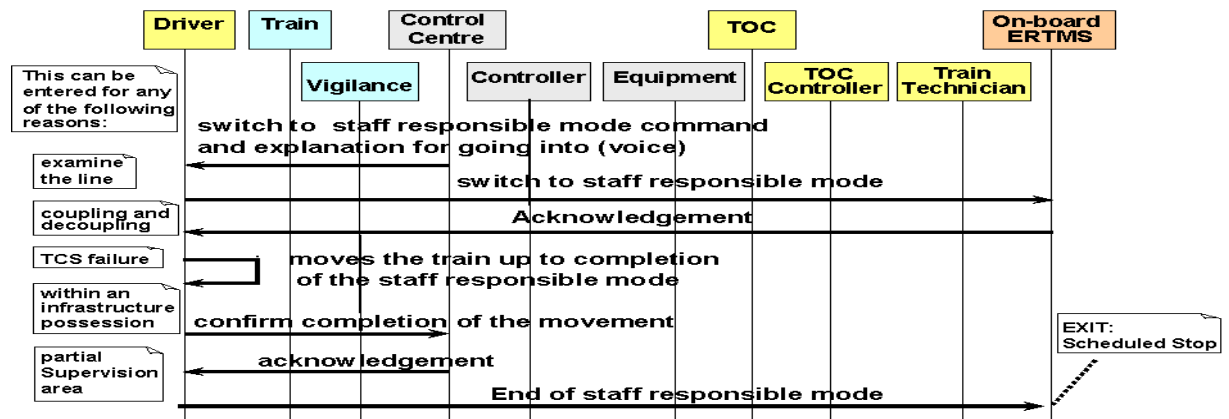


Figure 4-2: Authorised Movement - Staff Responsible [Sequence & Collaboration diagram]

All the actors/constituents of the system taking part in a states’ existence are positioned on the top of the diagram. The vertical axis represents time and horizontal directional lines define exchanges between the actors.

These exchanges can be communication or command/control exchanges and are distinguished by use of full and dotted lines respectively. Transition points (entry to the state and exit from the state, including transition triggers) have been described as well.

These representations have been used as a base of the hazard identification process.

Each of these exchanges has been analysed one by one.

4.2.4 Focus and Identification

Hazard Identification

Usually a Hazard Identification (HAZID) session is structured around loose system descriptions or system block diagrams. However in support of the HAZID for this project, the system scope and context was depicted using the State Transition and Sequence and Collaboration (S&C) Modelling. This novel use of existing modelling techniques, in support of the hazard identification resulted in a structured and systematic base for the hazard identification as the hazards resulting from each process or interaction were elicited (Lucic, 2005c). A common method by the consideration of keywords (such as NOT, LATE, EARLY, ALSO, etc) in relation to each exchange of

the S&C models was used to support the HAZID process.

In addition, a novel function of the context diagram was to identify the experience and expertise required from the hazard identification panel. Participants were allowed to express their opinion and encouraged to take an active part in the session.

In order to secure as comprehensive as possible source of data and ideas care has been taken to form groups with wide range of trans-national expertise:

1. Engineers with design experience;
2. Operation managers;
3. Maintenance engineers;
4. Performance and Safety Performance managers;
5. Safety & Standards managers;
6. Train drivers.

Identified hazards were carefully recorded to be used as the base of further analysis.

There are many benefits of “on-line” capture, the main one being that the panel can agree (or argue about, which is more usual) the final wording of the hazard and its consequences and mitigations. The form, designed in Microsoft ACCESS and projected on the wall during the HAZID sessions was used to capture all the elicited information.

Analysis of hazards

Around 150 hazards were identified. This is too many hazards to analyse individually and furthermore many are related anyway. Consequently all similar and/or related hazards were grouped into higher level groupings, clusters of hazards, labelled Core Hazards.

Core Hazards were the base cells of knowledge integrated into the knowledge structure. In a way, the Risk universe was partitioned into galaxies of hazards.

Initially, a “risk universe” with 10 “galaxies”, Core Hazards, was formed:

1. Less Restrictive Movement Authority;
2. Driver Exceeds allowable Movement Authority;
3. Train Exceeds allowable Movement Authority;
4. Inappropriate Routing of Train;
5. Errors & Failures during Shunting;

6. Errors & Failures during Rescue;
7. Errors & Failures during Coupling/Joining;
8. Errors & Failures during Shutdown/Power up;
9. Errors & Failures during Standby/Prepare for Next Mission;
10. Inappropriate Level Transitions.

However, some of the Core Hazards were too complex to be modelled, hence some of them were divided into a Number of Sub-Core Hazards. At the end 19 Hazard Groupings were established. Following the analysis of each core hazard, 40 Cause – Consequence models have been developed, because for some of the core hazards, more than one model was needed in order to adequately model the safety risk.

4.2.5 Core Hazards Modelling

Causal Analysis and Modelling is the first part of the modelling process. The aim of the causal analysis is to identify all the events/causes, and all the intermediate conditions which lead to a hazardous condition (Lucic, 2005d).

Each of the Core Hazards has been analysed in turn, attempting to determine all the causalities of the Core Hazard and logical relationships between identified causalities leading to the materialisation of the Core Hazard. As result of this, a fault tree has been developed for each Core Hazard.

In a fashion similar to causal analysis, consequence analysis of each core hazard has been undertaken. Consequence analysis involves establishing the intermediate conditions and consequences that may arise from a hazard. It involves bottom-up assessment of each hazard and is focused on post hazard horizon. At each intermediate state existing defences against potential escalation have been identified. The defence may be equipment, procedure or circumstance.

The sequence of identified intermediate conditions is termed “the hazard development scenario”.

The consequences fit into one of the following categories: predominantly safety related consequence, predominantly commercial consequence, predominantly environmental consequence, broadly safe condition.

The combination of a causal model of a core hazard and the consequence model, of the same core hazard, results in the Core Hazard Cause-Consequence Model. The model calculates the frequencies or probabilities of occurrence for all the consequences within the model.

To estimate the risk that each of the consequences brings to the system it is necessary to calculate the loss that each consequence may give rise to. To estimate the loss for each of the consequences a software based tool has been used, General Loss Estimation Engine (GLEE).

Loss for each consequence has been characterised through the following categories:

1. Safety loss to Passengers:
 - a. Minor Injury;
 - b. Major Injury;
 - c. Fatality;
 - d. Equivalent fatalities;
2. Safety loss to Worker:
 - a. Minor Injury;
 - b. Major Injury;
 - c. Fatality;
 - d. Equivalent fatalities;
3. Safety loss to Neighbour:
 - a. Minor Injury;
 - b. Major Injury;
 - c. Fatality;
 - d. Equivalent fatalities;
4. Commercial loss (damage to property);
5. Delays to service;
6. Environmental damage.

The tool is based on use of the accident data from European railways to calculate estimated cost of safety, commercial and environmental losses.

The tool provides separate cost calculations for each of the above categories and has integral treatment of uncertainty and modular structure providing a flexible and expandable environment. The tool works in two modes:

Site-specific: allows the user to fully specify the region in which the incident occurs,

including other input parameters such as types of train involved, time of day etc.

Network: the user is required to input only the type of incident and then the losses are calculated for averaged input parameters for a specified network (e.g. nationwide).

As result of that the risk prediction from the model is expressed in 15 categories corresponding to 15 loss categories as detailed above.

In order to support risk profiling, integration of individual core hazard models into one, overall safety risk model and options analysis, the existing technique cause consequence modelling was developed further as detailed in related sections below.

4.2.6 Model Data

Because the project was pan-European, inclusive of all European railways, the model had to take into account all the different system configurations across Europe.

Hence, the only pragmatic solution to the problem was to invent a virtual railway line, depicted by the parameters averaged (worst case from each line) across 5 European high speed railway lines.

Parameters identified as significant to our modelling have been normalised to produce the European Reference Operational Environment (Lucic, 2005d). Following is a sample of used parameters:

- | | |
|-------------------------------|---------------------------------|
| 1. Number of level crossings; | 5. Number of trains; |
| 2. Number of stations; | 6. Number of passengers; |
| 3. Number of signals; | 7. Average train weight; |
| 4. Average train speed; | 8. Number of trackside workers. |

These parameters were used to calculate failure rates for the model elements, base events and barriers. For example, a failure rate of a subsystem is a function of number of trains passed and their average speed and weight, or probability of worker protection procedures being successful is a function of the average train speed, number of trains passing and number of workers on the line.

Collated together the information about parameters forms a Parametric Data Set (PAD).

Following from that, a data set containing all the parameters used to calculate base event and barrier values has been defined.

The parameter values from the data set were “fed” into the model, the calculations were run and “Crisp value” absolute risk for each consequence was calculated.

4.2.7 Integration of Individual Models into a Holistic System Safety Performance

Model – Development

Initially individual Core Hazard models have been developed. However the reality does not consist of a number of standalone hazards. Clusters of Hazards, referred to as Core Hazards interact with each other defining all the properties of the “Risk Space”.

Hence, it was necessary to identify all the dependencies between the Core Hazards.

Some of the models where in fact, feeding into other models, defining the failure rates of higher level base events, or barriers as represented in Figure 4-3 below. Once all of the dependences were identified, the individual core hazard models were integrated into a “system safety performance model” (Lucic, 2005d).

In addition to the integration into a “system safety performance model”, it was concluded that grouping all the similar consequences together into a so called virtual consequence would be very useful; if the virtual consequences correspond to accident categories collated by industry or regulatory bodies since these can be used to calibrate the model against the historical data.

A simple criterion for grouping of consequences was developed specifically for that purpose:

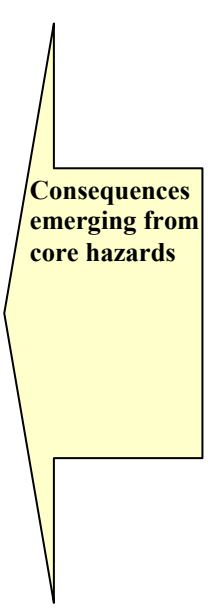
Total System Consequence	Level 4 virtual consequence	Level 3 virtual consequence	Level 2 virtual consequence	Level 1 virtual consequence	Real consequences
Σ of all risks	Safety Consequences	Train Accidents	Movement	Collisions	 Consequences emerging from core hazards
				Derailments	
				Level Crossing Accidents	
			Non-movement	In Stations	
				Other premises	
		Other (explosions, fires, structure failures, etc.)	Predominantly Passenger Related	NA	
			Predominantly Neighbour Related	NA	
			Predominantly Worker Related	NA	
	Commercial / Environmental Consequences	Train Accidents	Delays	NA	
			Infrastructure Damage	NA	
			Environmental Damage	NA	
		Other	Delays	NA	
			Infrastructure Damage	NA	
			Environmental Damage	NA	

Table 4-1: Consequence Groupings

Consequences emerging directly from the core hazard models were grouped simply, by summing all the same risk categories together. For example predictions for two consequences are:

1. For consequence “A”: 2 fatalities per annum, 5 major injuries per annum and 34 minor injuries per annum;
2. For consequence “B”: 4 fatalities per annum, 7 major injuries per annum, 55 minor injuries per annum and £2,000,000.00 of commercial damage per annum.

An integrated consequence “C=A+B” is: 6 fatalities per annum, 12 major injuries per annum, 89 minor injuries per annum and £2,000,000.00 of commercial damage per annum. The Total System Risk prediction is simply a sum of all the consequences together.

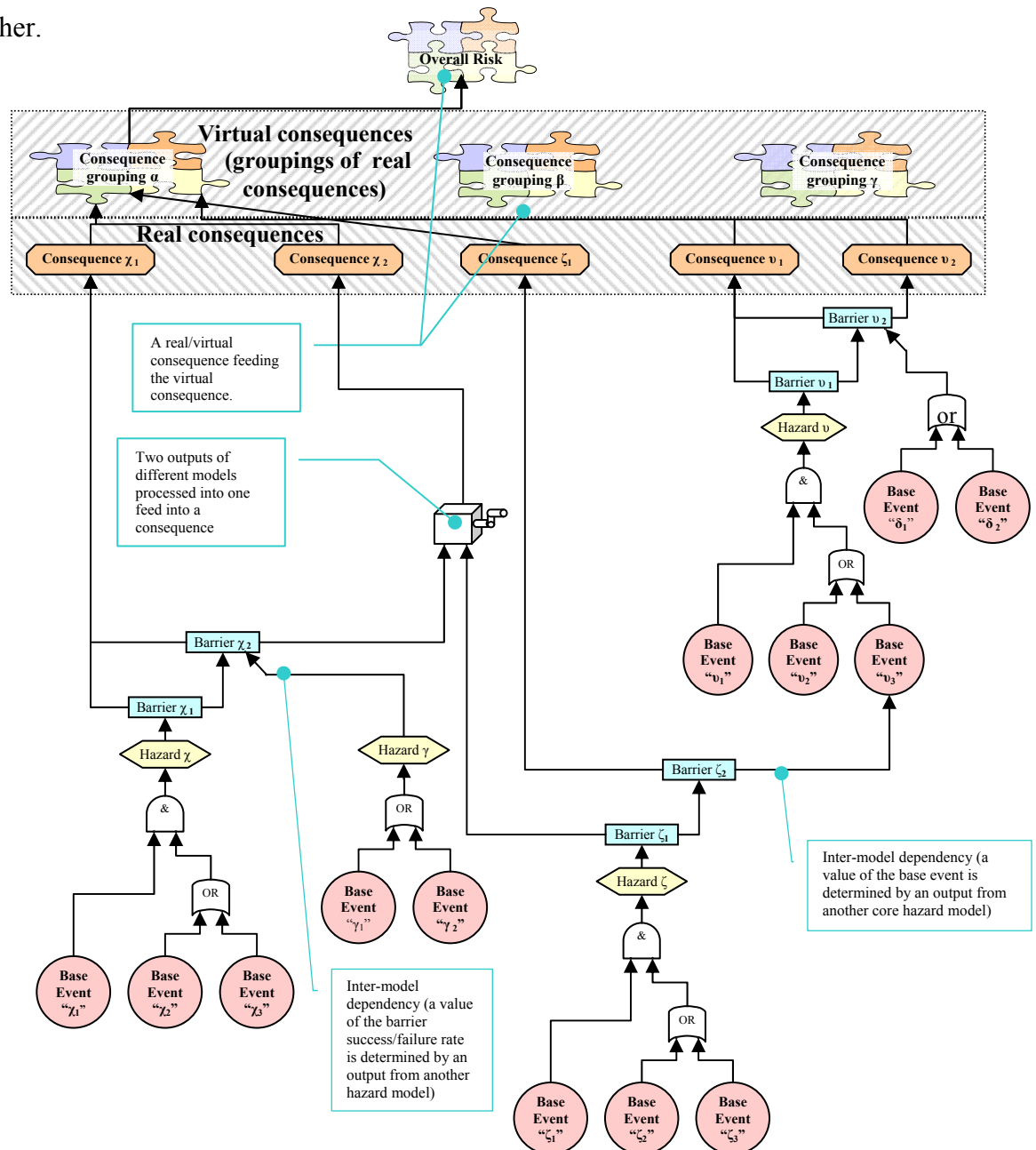


Figure 4-3: Core hazards models hierarchy

the author specified and carried out further upgrade of ISAE tool (Lucic, 2005e), assisting development of integrated/correlated models through introduction of new objects within the ISAE.

Four new functions and types of linking were identified during the integration process:

1. An output of one core hazard model determining the frequency of a Base Event, the constituent of another core hazard model structure. There are two possible ways that this link may happen:
 - a. A link between two models is established/identified to pass the frequency of the consequence originating from one model to the base event of another model (the information passed is the calculated frequency of the consequence). This frequency becomes the frequency of the base event occurrence;
 - b. A link between two models is established/identified to pass the frequency of the critical event originating from one model to the base event of another model (the information passed is the calculated frequency of the critical event). This frequency becomes the frequency of the base event occurrence;
2. A fault tree determining the probability of success of a barrier, within one model. Sometimes a barrier is defined by a combination of events. In that case a fault tree is required to describe and define performance of the barrier;
3. A real/virtual consequence feeding the virtual consequence. In the case of the linking between the models being established by linkage of real consequences into virtual consequences, the information passed from the real consequence should be calculated risk for each loss category;
4. Intermediate processing. Regardless of the type of the link, information carried by the link could be processed in several different ways:
 - a. Logical processing in terms of “AND” and “OR” logical operations performed on combined links;
 - b. Splitting of links into several outputs with distributed weighting;
 - c. Transform function performed on combined links producing single or multiple-weighted outputs;
 - d. Simple addition of multiple links of the same type into a single link.

Following from the above identified novel functions two different modelling environments were identified as well:

1. Individual models worksheets: Within this environment, modelling of individual models is carried out. Basic characteristics of this environment are same as the characteristics of the previous cause-consequence modelling environment, with

following exceptions:

- a. New inter-modal IN and OUT symbols were introduced, in support of integration and linking of outputs from one model to inputs into base events or barriers of other models;
 - b. Facilities to support three dimensional classification of base events were incorporated, as detailed later in section 4.2.10 Derivation of Requirements;
 - c. Enhanced apportionment engine was incorporated into as detailed later in section 4.2.10 Derivation of Requirements;
2. Model Integration Environment: This is a completely new working/modelling environment developed within the ISAE tool.

New objects “operating” within this environment are first listed below and described in detail in APPENDIX B:

1. Critical Event Model super object (real consequences and base events of the model) to enable graphical linking of models into an integrated super-model;
2. Transfer Function *intermittent operator*;
3. Splitter *intermittent operator*;
4. Logical Gates (AND, OR) *intermittent operator*;
5. Super Connectors *intermittent operator*;
6. Virtual Consequences;
7. Links from real/virtual consequence to virtual consequence;
8. Links from real consequence to base event;
9. Links from the critical event to the base event.

These additional objects are necessary and sufficient to support inter-modal integration process.

Inter-modal, model integration environment is illustrated by Figure 4-4 below.

Following integration of the Core Hazard Models, it was possible to calculate contributions of individual model elements to the total System Risk.

Overall the integrated model consists of 40 individual models, corresponding to 19 core hazards (some core hazards could not be analysed by a single model, and were broken into smaller, more manageable pieces referred to as sub-core hazards). In total the integrated model consist of 583 base events, 240 states, 499 barriers and 365 consequences.

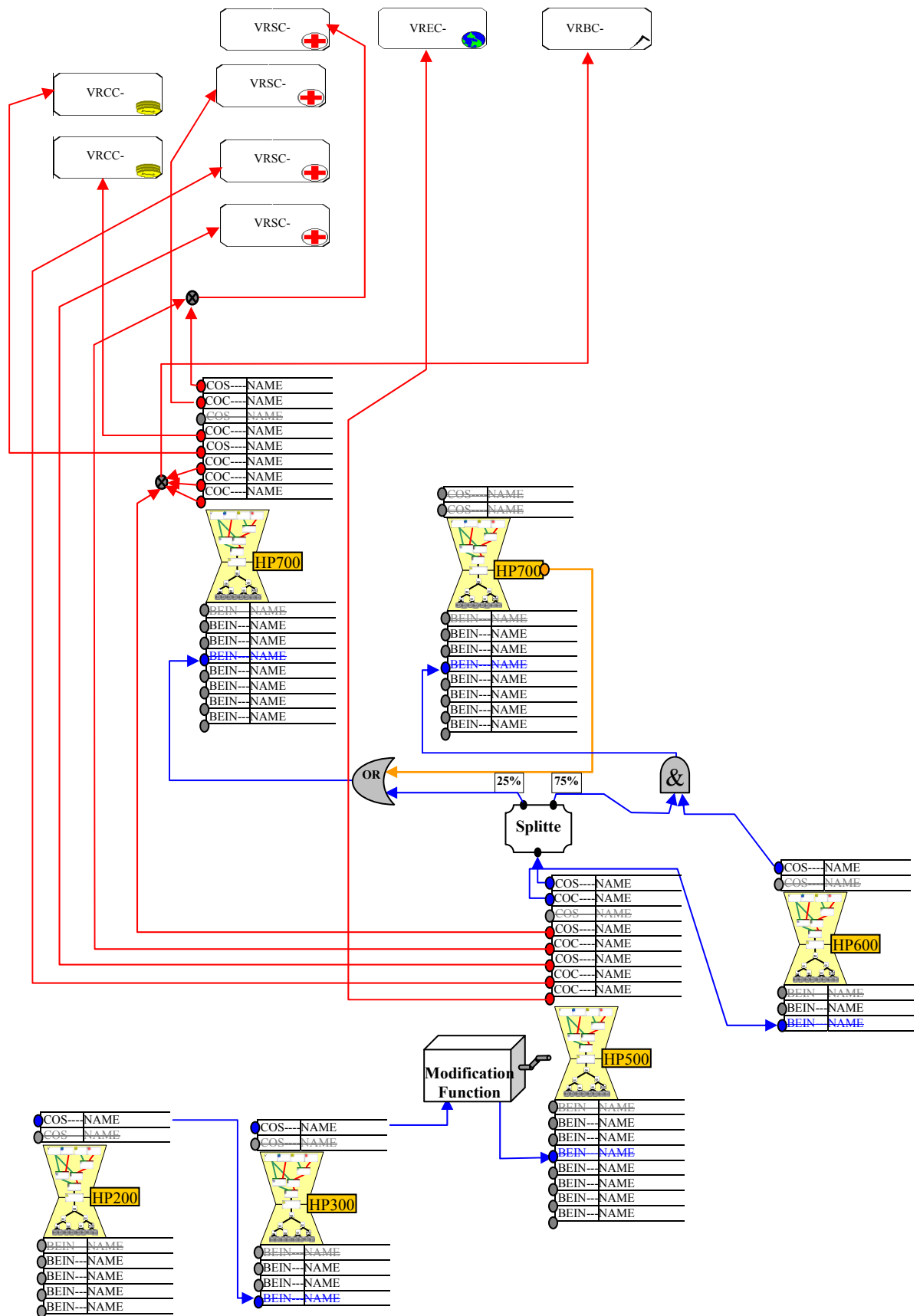


Figure 4-4: Model integration environment

4.2.8 Output Generation and Normalisation

The following is a sample of some of the forecasts:

Consequences		
Ref	Description	Annual Frequency
1.1	Collisions	2.6
1.2	Derailments	1.1
1.3	Other Movement Accidents	0.2
1.4	Commercial Only Accidents	1600
1.5	Null (no consequence)	2900
1.6	Level Crossing Accidents	0.00088

Table 4-2: Sample of ERTMS study result data

Thus the predictions are 2.6 collisions per annum, 1.1 derailment per annum, other movement accidents 0.2 per annum (or twice each 10 years), 1600 accidents resulting in commercial risk only each year, 2900 times nothing will happen though the hazard will exist (or in other words the accident will be averted) and 0.00088 level crossing accidents per annum.

Safety targets as stated by European Commission for Railways are (per year per exposed person):

1. Average population safety target → $1.0\text{E-}05$;
2. Passenger risk of fatality → $3.3\text{E-}06$;
3. Workers risk of fatality → $3.3\text{E-}06$;
4. Neighbours risk of fatality → $3.3\text{E-}06$.

Comparing the first forecasts against the above targets clearly indicates that the original model predictions for the safety performance of the system were unsatisfactory.

Comparison of virtual consequences against railway accident reports was used to calibrate the models against the historical data. The review of data and logic resulted in several corrections to the logic and data of the model, until a model was accepted as representative (Lucic, 2005d).

4.2.9 Risk Profiling

The first step towards risk profiling was to define the parameters not as crisp values but as statistical distributions, with minimum and maximum values and a distribution.

Consequently calculated risks are articulated as statistical distribution.

This type of risk profiling is referred to as “One Dimensional Risk Profiling”.

By defining the parameters as functions of time and space, the risk calculations become three-dimensional, distribution functions of time and space.

This type of risk profiling is referred to as “Three Dimensional Risk Profiling”.

4.2.10 Derivation of Requirements

Apportionment and Importance

Although risk profile is extremely useful, being able to identify the contribution of model elements, or in other words the contribution of equipment and procedural failures and human errors to the total risk is even more desirable. This process is referred to as “apportionment”.

The following problem was encountered on the onset of the apportionment study:

Base events and barriers actually represent failures of equipment and procedures, which in different scenarios cause different problems, thus what is required is to ascertain the absolute level of reliability of equipment and processes, necessary to achieve in order to produce a safe system. However, the integrated model is very large and complex, with many instances of the same equipment or process failure causing different consequences.

For that reason it was necessary to find a way to distinguish the model elements representing the same type of the failure.

As a solution to this problem a three tier classification system was introduced, differentiating between:

1. A function provided by the system or constituent (primary classification), for example Train Speed Control;
2. A function provider (secondary classification), for example Automatic Train Protection System on board of the train;
3. A function environment (tertiary classification), for example failures arising During Protected Movement.

Therefore, part of description of each model element (Base Event and Barrier) is its three parameter classification vector $\{x,y,z\}$.

For each classification group, primary, secondary and tertiary, a substantial number of classifications have been identified and the data on classifications is kept as a separate table depicting all the classifications and classification coding (abbreviations).

Combining tables of classification coding with data sets containing parameter values (or

functions) results in a data set referred to as a General Parametric Data Set (GPAD). The GPAD contains all the parametric information and classification descriptions feeding into the model.

Most of the configuration management of the model was concentrated on the GPAD. This is because once the model logical structure is developed and confirmed as a correct one, this part of the model becomes almost static and the changes introduced to the model are mostly related to changes of parameter values and classifications. The GPAD must be carefully configuration managed since a small change in one of the parameters may have large impact on the total risk prediction calculated by the model, and it is necessary to know to what data set the calculations relate. By simply changing the GPAD data it is possible, using the same logical structure, to simulate different system configurations. This is a great advantage, since until the system solution becomes stable, potentially many different system configurations are possible and representing each one separately through a direct change in the model would be extremely time consuming.

By adding together contributions of all the model elements with the same classification code, the overall contribution of individual equipment, groups of people or procedures to the total system risk was calculated using new algorithms developed in support of this modelling technique.

Analysis was performed on 4 different levels for each risk category:

1. Apportionment of a virtual consequence to lower layer virtual consequences feeding it;
2. Apportionment of a virtual consequence to “source” consequences;
3. Apportionment of a virtual consequence to Core Hazards (Critical Events);
4. Importance of a virtual or a “source” consequence relative to Base Events and Barriers.

The author developed algorithms for all 4 calculations as outlined in the APPENDIX A of the thesis.

Requirements

Estimating risks emerging from a system is useful but what is required is a target rate for each core hazard/sub core hazard or Tolerable Hazard Rates.

For each of the core hazards an annual rate that would satisfy the Safety Targets as specified by European commission for transport has been calculated. The hazard rate is expressed as an annual frequency of occurrence.

Following from that, the results of modelling were used to establish the target Safety

Integrity Levels (SIL) for Control Command Constituents (subsystems of the train control system). Using calculated minimum and maximum annual failure rates and probability values SILs were allocated to subsystems (Lucic, 2005f).

4.2.11 Optioneering application

The most beneficial use of the modelling is in support of options and impact analysis. Using the model it is possible to identify the most important contributors to the risk and concentrate efforts to improve the performance of the system on these critical model elements (Lucic, 2005f).

An important part of options analysis is apportionment to the model elements. As already mentioned earlier, it is possible to distinguish three apportionment categories:

1. Apportionment to failures of functions within the system;
2. Apportionment to failures of function providers and
3. Apportionment to failures of function providers operating in specific mode.

For example, apportionment of total equivalent fatalities to equipment (control command constituents) and subsequently to functions provided by each control command constituent (the model indicates that 17% of risk comes from the subsystem “L” (vital computer), where of total failures of vital computer 35% happen during data entry, 19% during start up and test, 18% during train trip, 14% happen when protection for passing trains is activated, 16% happen when external alarms are activated).

There are two ways to utilise the model for optioneering and impact analysis.

Firstly it is possible to change the parameters values and shape of distribution and see the impact of these changes on model predictions.

Secondly, a new base event or a barrier (a new model element) can be implanted and the impact of the change assessed.

In both cases of optioneering it is the impact of the change, from original risk profile to new risk profile that is being analysed. Using these results it is possible to justify either additional investment to implement new mitigation measure or improve performance of existing equipment or reasonably reject implementation of suggested mitigation measure using as an argument a line of reasoning fact that investment is grossly disproportionate to the benefits new mitigation measure could create if implemented.

4.3 Second Project: Axle Counter modelling

4.3.1 Purpose and Scope of the Project

In this section a risk modelling process as the author applied it on a real life project, from the initial stages of elicitation to final stages of testing and application is presented.

Axle counter application risk models have been developed aiming to support derivation of Safety Cases for individual axle counter installation projects. In accordance with the UK safety case regime, each project will have to prove that the technological and procedural solution accepted for the project is the As Low As Reasonably Practicable (ALARP) solution.

To achieve this, each individual project will have to demonstrate that a number of different options have been considered and that the most suitable solution has been selected. In addition to this, the project will have to prove that the safety risks introduced to the railway system by introduction of new technology are acceptably low.

In this section the focus will be on a model supporting analysis of the Reset processes, the Failures during reset model. The aim of this section is to:

1. Depict the development of Axle Counter Application Models;
2. Describe the process followed during the development of the models and;
3. Outline the process for future use of models.

4.3.2 Axle Counter Train Detection Concept

The overall behaviour of an axle counter is represented by the state-space diagram in Figure 4-5.

Essentially, an axle counter detects the passage of train wheels at the entrances and exits to a section of track, and increments or decrements a count accordingly.

If the count is more than zero, then the track section is set to occupied, and if less than zero the section is set to undefined. If the count is zero, and if internal safety checks, which will depend on the specific design of the axle counter in question, are satisfied, then the track section will be indicated as clear.

Thus, when the first wheel of a train entering the section passes over a detection point, the section will be indicated as occupied. As each subsequent wheel passes over the detection devices in the same direction as the first (usually called “counting heads”) the

internal count will be incremented. As the train leaves the section, the count will be decremented for each wheel that passes over the counting heads.

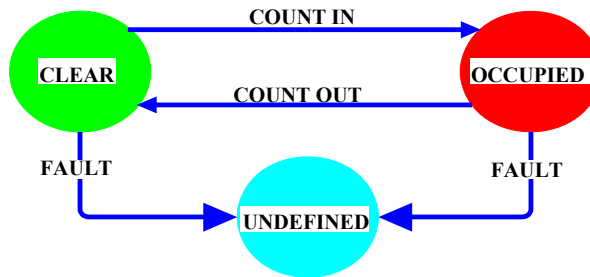


Figure 4-5: State-space diagram

When the last wheel leaves, the count will return to zero, and provided the internal safety checks have been satisfied, the section will once again be indicated as clear.

An important safety check, which is common in principle to all types of axle counter, concerns the detection of any event which could have interrupted the ability to detect and count wheels at any entrance or exit points. Such events might include interruption of the power supply, loss of communication with a detection point, or temporary removal of detection devices.

If such an event occurs, then it is possible that a train may have entered or left the section undetected, and it is essential that the axle counter should default to a non-clear state until it has been brought into correspondence with the actual state of the railway.

The default state, which is generally, designated the “disturbed” or “undefined” state of the axle counter, will typically be treated as equivalent to an occupied state by the rest of the signalling system.

Recovery from the disturbed state can normally be achieved only by the operation of an external reset control, although it may be possible with certain designs of axle counter for the recovery to be achieved automatically following the successful completion of a complete count in – count out cycle as a train occupies and clears the section.

The latter arrangement would be possible only for certain, very specific types of disturbance. The external reset facility resets the axle counter to a clear state on all types of axle counter considered to date.

4.3.3 The Modelling Technique and the Tool

The technique used for the development of the risk models is known as Advanced Cause-Consequence Analysis and is described in previous section. The tool used for development of these models is Integrated Safety Assurance Environment 8 (ISAE8). The Integrated Safety Assurance Environment assists development of Cause-

Consequence risk models by organising the input, ensuring that all details captured are recorded, and allows the analysis of models using graphical worksheets.

Once the models are complete, ISAE8 can then generate a mathematical model and will allow different scenarios to be run to assess the influence of different factors on the model.

Whilst ISAE8 is a good analysis tool, it must not be the basis on which decisions about life and death situations should be based. However it does provide an insight into the model, and may focus the further studies and analysis required.

The ISAE8 system is split into three distinct areas:

1. Pre-Processing;
2. Core Functions;
3. Post-Processing.

Pre-Processing: includes all the functions required to set up the project management information and the initial data collection. The following are constituents of the Pre-Processing module of ISAE:

The Hazard Log, should be used initially to record information about the Hazards.

The System Parameters. The tool supports parametric modelling (numerical values of model elements can be expressed as fixed numbers, parametric functions or statistical functions. This module of the tool allows for information about parameters to be defined. Sets of parameters can be organised in different Parametric Data Sets, corresponding to different scenarios to be modelled.

The Classifications. As the risk analysts construct the model, additional data is captured at significant points in the design in the form of classification codes. When the model is complete the models can be calculated based on the apportionment of risk based on these classification codes. So when preparing ISAE for use in a new project, it is important to enter the Classification Codes early in the process to be used should be entered in the system.

The management side involves setting up and maintaining information about:

1. Organisations involved in the project;
2. The hazards within the project;
3. The project team;

4. Project documents;
5. Project tasks.

Core Functions: includes the main Causal and Consequence modelling element of ISAE and allows the user to produce a risk model using various building blocks (Base Events, Logical Gates, Critical Events-Hazards, Barriers and Consequences), which can be drawn onto one or more Worksheets to model the Hazard. Once the risk scenario has been drawn it is validated and an Excel compatible Algorithm File (ALF) can be generated for subsequent simulation. It is also possible to define formulae for the losses pertaining to each Consequence or Accident. The Core Functions module also supports integration of models of individual hazard scenarios into one integrated, holistic model.

Post-Processing: allows further evaluation of the risk model by generating “What-if” scenarios. It also includes a reporting facility and the apportionment function to calculate the risks apportioned to selected elements.

Accurate and reliable train detection is an integral part of a safe railway signalling system. The principal method of train detection, in the UK, has been by the use of track circuits.

The widespread introduction on the UK Railways, of axle counters for train detection where track circuits would otherwise have been used, is a strategic decision made by the Network Rail (UK Railways custodian).

Axle counters have only been used in specific applications in the UK, generally in small quantities. The large scale, widespread application of axle counters is new to the UK railway industry.

The Concept Safety Case (ATKINS, 2002) was developed to demonstrate that axle counter systems can be implemented safely on Network Rail controlled infrastructure where track circuits would otherwise have been used.

The Concept Safety Case does not attempt to show that risks associated with axle counters are ALARP in an absolute sense. It does show that the risks associated with axle counters can be made as low, or lower than, those associated with track circuits.

It provides a framework so that individual application safety cases can demonstrate that the type of axle counter system that is being commissioned on a particular project reduce the risks to ALARP (relative to provision or retention of track circuits).

Application specific issues cannot be addressed at the concept level. To demonstrate ALARP, it is necessary to consider the application in conjunction with the Concept Safety Case, as the latter cannot deal with reasonable practicality in all situations.

What is reasonably practicable is dependent on the specific technology of the axle counter, and of the signalling system of which it forms part, and the specific circumstances of the application.

Thus, provided individual Project and Application Safety Cases demonstrate that they have met the safety targets, the integrity requirements and the generic safety requirements provided within the Concept Safety Case, and that they have mitigated the specific project and application hazards, the Project Safety Case demonstrates that axle counters can be used safely as the sole train detection system where track circuits would otherwise have been used on Network Rail controlled infrastructure (ATKINS, 2002).

There are many factors to consider on UK railways infrastructure, all of which vary considerably throughout the UK:

1. Traffic density;
2. Rolling stock;
3. Traction systems;
4. Procedures;
5. Clearances; and
6. Control systems.

Consequently the model developed to support individual axle counter projects, had to be generic, independent of any particular project solution and application but capable of simulating the particular project solution and environment.

4.3.4 Analysis Approach

Scope of analysis and modelling included all interfaces between the signalling system and the axle counter system, taking into account all the processes related to axle counter operation including control, command and communication exchanges.

Capability to realistically represent any chosen application is achieved by complete separation of logical structures and underlying data.

By changing the dataset used to run model calculations it is possible to simulate different, project specific solutions.

The process adopted for the development of models consists of 7 stages:

1. Review of existing related information;

2. Definition of the system;
3. Identification of hazards;
4. Analysis of hazards in terms of grouping and structuring;
5. Cause-Consequence analysis - Development of logical structures;
6. Cause-Consequence analysis-Parameterisation;
7. Testing, reviewing and gathering of data for testing.

The high level overview of the signalling system has been developed in support of the identification of hazards and options for mitigation of hazards. The signalling system overview used as a base for hazard identification and modelling, defines all potential interfaces between the signalling system and the axle counter system, taking into account all the processes related to axle counter operation including control, command and communication exchanges.

The main elements of an axle counter and the associated parts of the overall system are shown in Figure 4-6. The following are the primary interfaces with the axle counter system:

1. The rails;
2. Train wheels/axles;
3. Communications. [Note: the communications system(s) may or may not be part of the Axle Counter System but are be considered to be part of the train detection system];
4. Human Machine Interfaces (HMI), that provide the Reset/Restoration requests/commands and an indication of the status, (occupied, clear or undefined) of the track section and diagnostics;
5. Interlocking / signal controls including level crossing controls;
6. The power supply.

The operational environment for axle counters has been developed and is described by the “Typical operational environment and Application Diagram for Axle Counters” (Lucic, 2004a). This description includes all the elements of an operational environment; structures, passengers, staff, constituents of the signalling system, environmental factors, railway neighbours and their infrastructure, constituents of telecommunication and electrification systems and trains and engineering machinery.

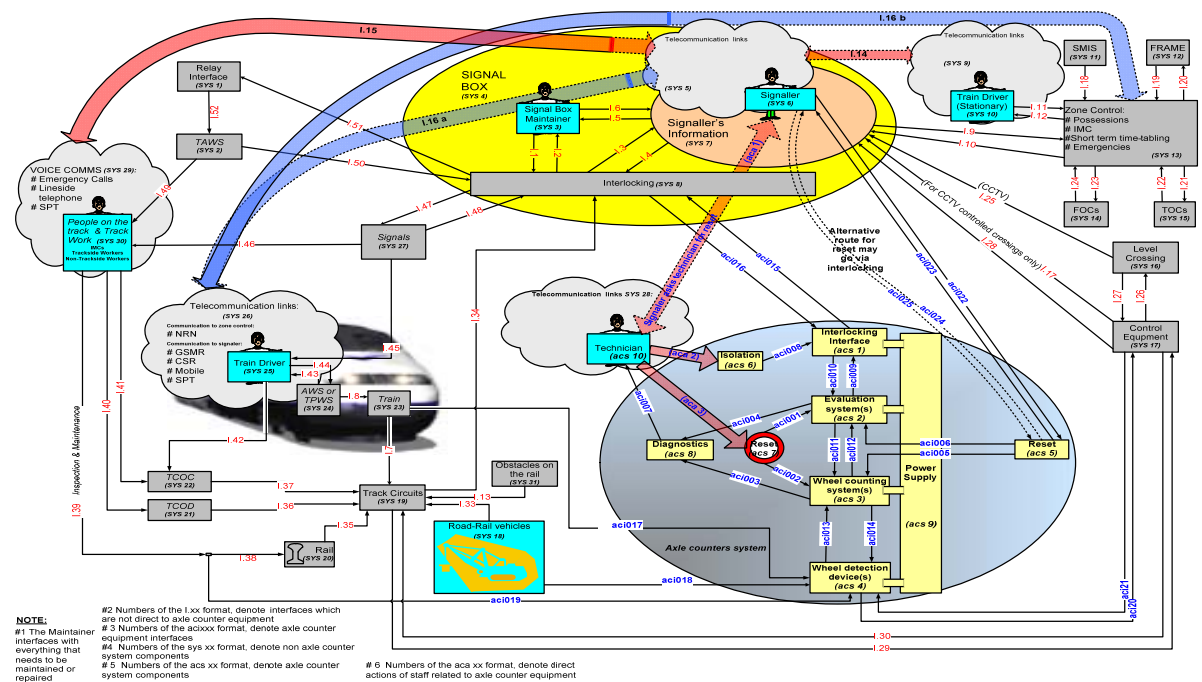


Figure 4-6: Axle Counter System

Identification and Analysis of hazards

Extensive and systematic hazard identification has been carried out based on the system description and description of operational environment (Lucic, 2003b). All of the hazards identified during the hazard identification study have been analysed, structured and mapped to the Core Hazards (higher level hazard groupings) originating from the Axle Counter Concept Safety Case aiming to support development of Cause-Consequence models for the project.

Two Core Hazards have been identified as related to the process of resetting the Axle Counter section:

1. Failures during reset (excluding level crossings);
2. Failures during reset (on level crossings).

Within the two core hazards clusters of Causalities and Defences have been identified. These were further analysed during the modelling stage of the project.

Model logic development

Risk models have been developed aiming to support any individual axle counter project. Consequently models' logical structures are generic, independent of any particular project solution and application (Lucic, 2004a).

Capability to realistically represent any chosen application and vary any relevant parameters is achieved by complete separation of logical structures and underlying data.

By changing the dataset used to run model calculations it is possible to simulate different, project specific solutions. Cause-Consequence models developed for this project can be separated in two discrete but completely integrated parts:

1. Cause-Consequence trees (logical structures);
2. Parameterisation of logical structures.

The models have been developed with the aim to support comparative safety analysis of different procedural and technological options for implementation of axle counter technology on different projects.

The models are inclusive of all potential system solutions.

The following are areas where different options that may affect the outcome are likely:

1. The nature of the reset/restore procedure used;
2. Type of technical controls involved in the process;
3. The nature of the signal aspect given to the driver of the "next train";
4. The requirement for the signaller to apply protection to the section to be reset should occur before the reset, but has an effect when the incorrect reset has occurred;
5. Availability of different types of communication means between the train driver, signaller, technician and other railway staff.

Fault Tree methodology has been used for causal analysis. The causal parts of both models are almost identical, the only difference being a model element calculating the proportion of hazards happening on the level crossing section.

The fault tree is structured in three main branches:

1. The elements resulting in a failure whilst attempting to reset a section with more than one section requiring reset;
2. The elements resulting in a failure whilst attempting to reset a section with only one section requiring reset;
3. The elements resulting in a completely unintended reset of a section.
4. The consequence parts of the two models are different. For the model of “Failures during reset (excluding level crossings)” the Consequence tree is structured in three main branches:

5. Occupying train moving on plain line;
6. Occupying train moving at points;
7. Occupying train not moving.

The structure of the “Failures during reset (on level crossing)” model is very simple. If the section controlling the level crossing has been incorrectly reset then the outcome depends on the presence or absence of road traffic and on the actions of the road user and/or the driver of the "occupying train".

The model covers all types of level crossings - the likelihood of a particular level-crossing being affected by the reset of the axle counter and the potential to warn the driver of an approaching train that the crossing is not protected.

For each model element, detailed descriptions are provided within the modelling tool environment. The frequency of occurrence of the hazard is measured in "number of incorrect resets per year" or frequency of failures during reset per year (how many times an occupied section has been reset each year).

Parameterisation

The use of parameterisation allows generic risk modelling of the Axle Counter Application. Whilst, Cause-Consequence trees have been developed to include all potential operational and engineering solutions to the application of axle counters in any geographical area, ease of customisation of models to a geographical area or a project is achieved through parameterisation (Lucic, 2004a).

Parametric functions are used to evaluate numerical values (frequencies of occurrence and probabilities) of all the model elements. Parametric functions replace the crisp values for frequencies and probabilities of occurrence/failures of base events and barriers.

Numerical values of parameters within the parametric expressions are defined within the data-set. This technology allows for an easy and auditable way of changing the base data for the model and recalculation of estimates for different variations of the source data.

Data-sets are defined as lists of parameters used to calculate numerical values of model elements.

Parameters depict numerical values arranged in a number of data-sets describing different parts of the railway. Therefore, when the model is to be calculated, prior selection of the data-set to be used is necessary.

This approach allows for increased flexibility in use of the generic model's logical structure. It also removes many of the undocumented assumptions hidden within fixed values that could result in an imprecise application model.

Parametric functions and data sets are used to analyse effects of the timetable related variations in operational performance, analysed scenario evolution elapsed time and spatial variations affecting the operational performance.

Some of the parameters, such as average headway and average speed, are related to the timetable and topology of the analysed route.

These parameters, if taken across the large area of the network, as the difference between the minimum and maximum values of the parameter increases, introduce significant margins of uncertainty.

If parameters such as average headway and average speed, averaged across large area, are used to support the modelling, modelling outputs will be of sufficient quality to permit coarse estimation of risk fluctuation caused by replacement of track circuits by axle counters.

It also allows for elapsed time to be taken into account as values of relevant model elements are calculated by the parametric formulas containing elapsed time parameters.

The project only considered model structure and data issues and any inter-dependencies between these in so far as was necessary to derive review and test the parameterisation.

The main deliverable was the model database populated with parametric expressions, rationales for these expressions and parameter definitions.

The overall parameterisation methodology is illustrated by Figure 4-7. This methodology is described in detail as follows:

I. Initial Review of Models and Documentation:

A review was carried out of the models and relevant documentation including the Axle Counter Concept Safety Case and the Axle Counter Template Application Safety Case.

II. Criteria:

The aim of this model development work is to allow the axle counter risk models to support the safety arguments in the axle counter template application safety case.

The documents reviewed above were used in the development of these criteria.

III. Workshop:

Having developed a set of criteria, a workshop was held to review the set of models.

IV. Model Update:

The models underwent a series of model updates. These formed the input for the next phase of model review.

After each model update, the model was reviewed and parametric expressions developed.

A record of all the changes to the model is kept.

V. Development of parametric expressions:

Parametric expressions were developed based upon a review of the model structures. A rationale for each expression was drawn up and is given as part of the model element rationale.

VI. Parameter List:

A list of each of the parameters used in the formulae together with their definitions and units was produced.

This underwent a number of review stages to ensure that the parameter descriptions were at an appropriate level of detail. However it should be recognised that for some parameters, (particularly those which are simply a statement of a base event or barrier probability) a complete understanding of the scope or context of the parameters can only be provided by reference to the model structures.

VII. Testing:

Testing of expressions is described in more detail in the following paragraphs of this paper (Lucic, 2003c).

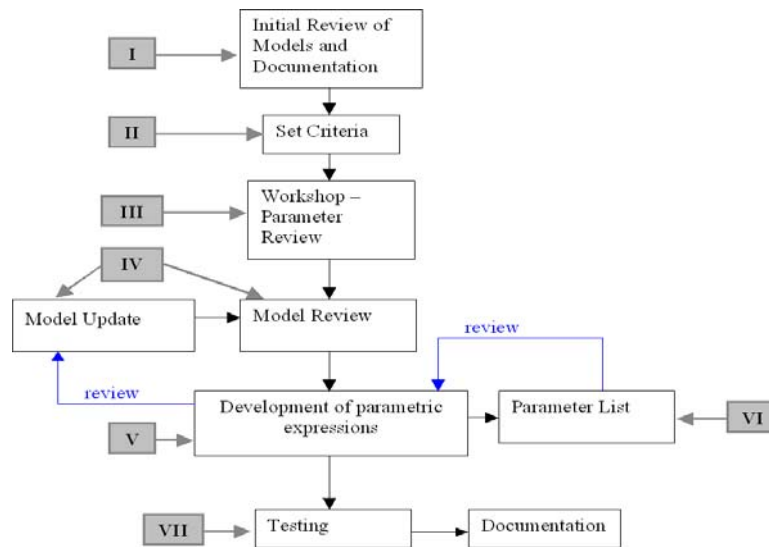


Figure 4-7: Parameterisation methodology

The parametric expressions were developed based upon the model review. A rationale for each expression was drawn up and is given as part of the model element rationale. These were entered into the model database together with the formula rationale. For consistency any parameter that represented a probability of success or failure was worded to represent failure.

Parameter units were made consistent and are as follows:

Time: hours or years; and

Length: kilometres

4.3.5 Tests

The complexity of the models developed during the modelling enhancement project, dictated structured and comprehensive testing (Lucic, 2003c). Testing of models encompassed the following model constituents:

1. Parametric Functions;
2. Logical Structures;
3. Model Predictions;
4. Data.

The required tests can be grouped into two categories:

1. Tests performed prior to application of models to the particular project, encapsulating testing of Logical Structures and testing of Parametric Functions of the generic models;
2. Tests to be performed in preparation for and as part of application of models to the particular project, encapsulating testing of Model Predictions and testing of Data.

In support of thorough and auditable testing of models, a Test Plan has been developed. Firstly, as part of the models' development process, all models have been reviewed by domain experts at different stages of the project.

The final version of models' logical structures has been agreed between all involved as accurate presentation of reality. However, further reviews of models should take place prior to their application on each specific project.

A second set of tests concentrated on Parametric Functions. The aim of these tests was to ensure mathematical correctness of the Parametric Functions and eliminate logic errors in their definition. The data for these tests was supplied by Network Rail. This data is a coarse estimate of possible parameter values and expected values for some model elements (Base Event, Barriers, Critical Events and Consequences).

In the absence of real life data, either for a specific application or for expected results, the aim of testing was to show that the result calculated by the formulae is of the right order. The format of this data was as follows:

1. For each data item a logical Minimum value has been estimated;
2. For each data item a logical Maximum value has been estimated;
3. For each data item an average value has been estimated as a range.

Subsequently, each model has been run using the above-described data sets. Any mathematical or logical inconsistencies discovered have been resolved or explained.

Results of these calculations have been compared against estimated expected values for model elements whose values are calculated by parametric functions (Base Events, Barriers, Critical Events and Consequences). All inconsistencies discovered have been resolved or explained.

For each future application of models to the real project additional tests should be carried out to ensure correctness of models with regards to the particular application. These tests should be based on coarse project specific data elicited for testing purposes only. The data should be a coarse estimate of possible parameter values and expected values for some model elements (Base Event, Barriers, Critical Events and Consequences). The format of this data should be as described above.

Subsequently, each model should be run using the above described data sets. Any mathematical or logical inconsistencies discovered should be resolved or explained and documented.

Final tests should be carried out using real life data collected in support of a specific project.

In addition to this, a number of model elements calculated by parametric functions (States, Barriers, Critical Events, and Consequences) should be identified and where possible, values for these should be ascertained based on historical data or estimates. Subsequently, each model should be run and the results of these calculations should be compared against the historical/estimated data described above. Any mathematical or logical inconsistencies discovered should be resolved or explained and the process should be documented.

When applying models to a particular project, whenever possible, the data for modelling should be obtained from multiple sources and the best quality data should be used for the analysis.

However, some of the parameters needed for analysis are not readily available and will have to be estimated. In order to assure consistency of certainty boundaries for estimated parameters, it will be necessary to specify a common approach to estimation of parameters of similar nature, for example all parameters related to human performance beings should be estimated using the same carefully specified process.

4.3.6 Application

Following completion of all the above described tests, gathering of data for a specific project was carried out. The first use of the models has been for analysis of different options for reset of an Axle Counter controlled Signalling Section after planned maintenance (Lucic, 2005a). Simulation of different options has shown significant differences in safety risk. Two options have been simulated.

The first option involves removal of technical protections of the signalled section that has been reset after maintenance. This option assumes that the first train coming along after the completion of the maintenance and reset of the section will enter the section without any technical caution. Following model elements have been affected by the first option:

1. Protection not properly applied before reset;
2. Route set for next train through affected section;
3. Driver of next train not cautioned;
4. Driver shown a special aspect;

5. Driver shown a red restricted by interlocking aspect;
6. Driver shown yellow restricted by interlocking aspect;
7. Driver pass auto signal at red but not cautiously;
8. No examination of the line with next train through (after maintenance).

The second option is introduction of an unconditional reset facility to the system.

Unconditional reset facility provides means for a reset of axle counter section without any hardware or software self checking measures.

Only one model element, “unconditional reset facility used” is affected by this option. In both cases, procedural protections will be introduced to ensure that the section is clear (not occupied by trains, engineering vehicles, tools or other large objects) prior to reset and removal of protections protecting the section.

Models have been run for three different sets of data:

1. Baseline data set containing data gathered during a number of structured workshops for a specific project;
2. Data set based on the baseline dataset reflecting implementation of the first option described above;
3. Data set based on the baseline dataset reflecting implementation of both, the first and the second option described above.

Comparison of relative change of hazard and consequence frequencies related to changes being assessed shows increase in safety risk of two orders of magnitude.

In order to support the options analysis further, sensitivity analysis on the models should be performed to identify the model elements which contribute most to the risk. These are the model elements the most worthwhile to focus the analysis with aim to improve the safety performance of the system.

These models have been developed to the point of test application. Prior to use of models for any project testing of the models on the project should be carried out in accordance with the testing specification.

For each individual project test plan should be prepared. Sensitivity or importance analysis should be used to identify those model elements for which the overall risk is most sensitive and particular emphasis placed on the testing of these model elements. The parameters that are very hard to estimate accurately should be identified.

In order to assess the impact that accuracy of these parameters has on the overall risk, importance analysis should be undertaken. Particular emphasis should be placed on derivation of the critical parameters. Derivation of barrier probabilities should always be done using the model structures as an aid to analysis.

Use of graphical models increases transparency of modelling and enables the user to see all the factors, which define the numerical values (failure rates/probabilities or frequencies/probabilities of events occurring) of model elements.

Parameters that define the barriers are contextual and conditional in nature, and it is necessary to pay attention to the context of a barrier and related parameters during the data elicitation process.

4.4 Third Project: Complex Railway Project Safety Management – Manchester South Capacity Improvement Project

4.4.1 Purpose and Scope of the Project

The Manchester South Capacity Improvement Project (MSCIP) was being undertaken as part of the West Coast Management Unit (WCMU) programme of works, with the purpose of providing additional capacity by upgrading the railway infrastructure in the South Manchester area. It was a multi-discipline Alliance Project covering track renewals and realignment, overhead line equipment renewals, power supply renewals and changes and resignalling.

The project was realised in a number of stages:

1. The Stage A work was a ‘Technology Demonstrator’ for the application of the novel Italian signalling system, never before used on the Network Rail infrastructure. This stage was commissioned in April 2003;
2. The Stage A+ works built on Stage A with the implementation of Train Protection and Warning System, and formed the next stage of the phased implementation of the signalling system. This stage was commissioned in December 2003;
3. The next phase was the Sandbach/Wilmslow (SHWW) Phase 1, with the purpose to close out Stage A/A+ issues and de-risk the SHWW Phase 2 stage, which followed;
4. When the SHWW Phase 2 stage was commissioned in summer 2006 the new signalling system was still not fully operational but main functionalities were provided;

5. Final commissioning took place in spring 2007, with the complete set of functionalities provided as planned.

A Project Definition Document and an Outline Project Specification were developed aiming to define the scope of each project phase.

4.4.2 Concept of Change Management

Each project has a duty of care to show that the railway as delivered is safe and to do this and show that it has been done, must subject each change to the railway system to safety analysis. However these changes vary enormously in significance, so safety analysis processes must be scaleable. The initial remit for each stage of the project will require the Project to make certain changes to the railway.

As the stage proceeds, changes may be made to the remit as part of a formal change control process.

The total change made to the railway is a combination of the two as the following diagram illustrates:

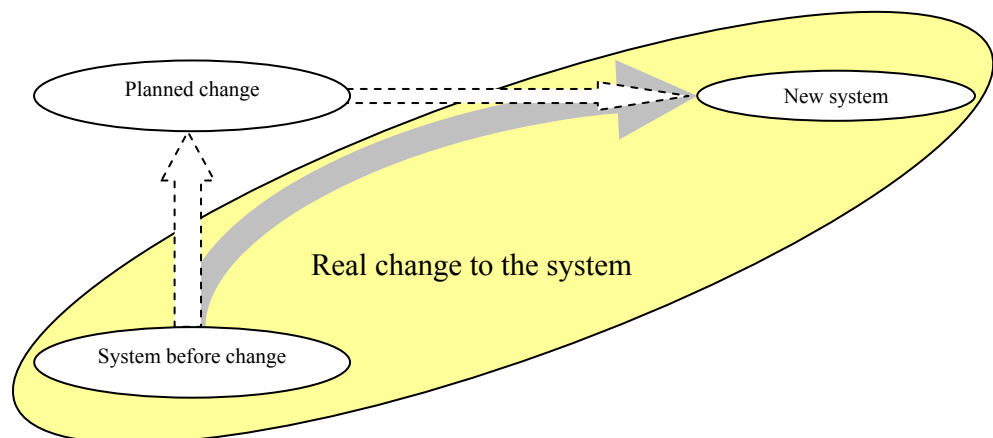


Figure 4-8: Concept of change

The safety analysis process for the project applies to:

1. All changes to be made to the railway which are defined in the initial remit for a project stage;
2. All changes subsequently made to that remit. These are typically described in Engineering Change Requests (ECRs). However the procedure also applies to non-engineering requests, such as proposals to change maintenance regimes, which may be documented elsewhere or records within the DRACAS.

The analysis focused on identification of novel interfaces and their further safety analysis, where novel interfaces are defined as:

1. Interfaces between novel equipment;
2. Interfaces related to or controlled by novel procedures;
3. Interfaces between conventional equipment but operating within the novel environment;
4. Interfaces related to or controlled by conventional procedures equipment but operating within the novel environment.

All the interfaces are initially classified into one of four levels of safety significance. This process is referred to as Initial Change Safety Analysis (ICSA).

The process categorises each change into four categories by safety significance, as follows (Lucic, 2003d):

- Category 0:** No hazards;
- Category 1:** All hazards controlled by existing standards or existing Hazard Log mitigations;
- Category 2:** Interface is novel but sufficiently simple and conventional that hazards can be analysed with reference to experience with existing equipment;
- Category 3:** Significant complexity and/or novelty.

Category 0 and Category 1 changes do not require safety analysis and a generic process is defined for Category 2 changes. Category 3 changes have to be analysed according to their specific attributes.

The process of analysis of Category 2 and Category 3 changes is referred to as Change Safety Analysis (CSA).

Detailed process is explained below.

Category 0 Changes: The Entry Criteria, Safety Analysis Process and recording requirements for the Category 0 changes are presented in the table below:

Category 0 Changes	
Entry Criteria:	No credible condition or scenario can be identified in which the process of making the change or the changed part of the railway could contribute to an accident. This is a strong criterion, which even very straightforward changes may fail, but will certainly apply to changes to the remit which do not

Category 0 Changes	
	affect the railway at all – for instance addition of a requirement to carry out a study.
Safety analysis:	None.
Records:	Reasons for categorisation.

Table 4-3: Category 0 Changes

Category 1 Changes: The Entry Criteria, Safety Analysis Process and recording requirements for the Category 1 Changes are presented in the table below:

Category 1 Changes	
Entry Criteria:	All hazards related to the process of making the change or the changed part of the railway are satisfactorily mitigated by authoritative good practice (such as Railway Group or Network Rail Company Standards) or by existing provisions of the System Hazard Log and the mitigation measures defined are being put into practice.
Safety analysis:	None.
Records:	Hazards; mitigation measures (by reference to authoritative good practice or the Hazard Log); confirmation that these mitigation measures are being put into practice.

Table 4-4: Category 1 Changes

Category 2 Changes: The Entry Criteria, Safety Analysis Process and recording requirements for the Category 2 Changes are presented in the table below:

Category 2 Changes	
Entry Criteria:	The change is of small or moderate complexity and all hazards related to the process of making the change or the changed part of the railway are sufficiently similar to hazards in existing railway equipment that they can analysed with reference to experience with existing equipment.
Safety analysis:	A Change Safety Analysis Briefing Note should be prepared containing: 1. A description of the functionality of the change; 2. A description of the physical configuration of the changed part of the railway;

Category 2 Changes	
	3. A description of the context of the changed part of the railway, identifying people, systems and equipment with which the changed part will interact. A Working Group with sufficient knowledge and expertise should assess the safety implications of the change. The Working Group should analyse the change as follows: 1. Confirm that the change is correctly categorised and that the Group has sufficient competence to analyse it; 2. Review the System Hazard Log to identify previously defined hazards or hazard causes which relate to the change; 3. Review the intended functionality of the change to identify hazards or hazard causes which could arise from correct operation or plausible deviations; 4. Review the physical configuration of the change to identify hazards or hazard causes which could arise from failure of the constituents; 5. Review the context of the change to identify hazards or hazard causes which could arise from interactions between the change and its environment; 6. Identify from the System Hazard Log, the description of the change and knowledge of the existing railway, measures planned or in place to mitigate hazards or hazard causes identified; 7. Assess the adequacy of these mitigation measures and, if necessary, propose additional ones. The process should be recorded in a Change Safety Analysis Report and the System Hazard Log should be updated in line with the Change Safety Analysis Report.
Records:	Change Safety Analysis Briefing; Change Safety Analysis Report.

Table 4-5: Category 2 Changes

Category 3 Changes: The Entry Criteria, outline of the Safety Analysis Process and recording requirements for the Category 3 Changes are presented in the table below:

Category 3 Changes	
Entry Criteria:	Any change which does not meet the entry criteria for levels 0, 1 and 2.
Safety analysis:	The scope of hazard analysis activities related to Category 3 changes is to be defined for each change individually. Following information for each of the hazards should be collected prior, during or after the hazard

Category 3 Changes	
	analysis activity: 1. Reference to the hazard analysis undertaking; 2. Reference to the system/sub-system/interfaces being analysed; 3. Reference to a life-cycle stage or stages that the hazard is applicable to (e.g. a life-cycle should be precisely defined within the briefing documentation); 4. Hazard item identification number; 5. Hazard item description; 6. Description of causes of the hazard item; 7. Description of consequences of the hazard item; 8. Action related to further investigation of a hazard item (if required); 9. Additional comments; 10. Nominated authority/owner of the hazard (where it can be ascertained); 11. Reference to the analysis Briefing Note for Category 3 change including the following: 12. Session title; 13. Description of the system to be analysed (with clear definition of session boundaries/interfaces); 14. Description of all assumptions made; 15. Clear indication of the scope of the hazard analysis undertaking (including reference to the life-cycle and system states); 16. Explanation of the process and structure of the session including the clarification of the terminology to be used; 17. Competencies and expertise required for undertaking the session; 18. List of participants including an outline description of their expertise.
Records:	All hazards identified through hazard identification activities, as well as any hazards recorded/transferred from other sources (and where accepted by the Hazard Manager) must be recorded within the System Hazard Log.

Table 4-6: Category 3 Changes

Cross references between the System Hazard Log entries related to novel interfaces and the system description were maintained.

A Project Definition Document (PDD) was reviewed and ICSA was carried out for all the changes planned for the project phase. Proactive safety analysis activities were then carried out for all the Category 2 and Category 3 changes.

CSA was carried out on all changes in the PDD; these were split into two and analysed as separate activities. Changes/novelties analysed during the CSA were identified as differences between the railway system configuration corresponding to the previous phase of the project and the current one. However the identified changes were then analysed against the standard railway system as a reference.

All CSA (Lucic, 2003d) activities covered operations under normal conditions, degraded mode and emergency conditions (where appropriate), from a wider point of view, inclusive of transitions from and to the operational mode. While the boundary of the CSA was defined as the boundary of the project scope, the CSA activities also considered the operational interfaces with adjacent control areas, maintenance and emergency services.

As part of the activities, a review was carried out of the impact of changes to be introduced by a new phase of the project on the existing mitigations (identified and implemented during previous project phase) aiming to confirm the validity of these mitigation measures.

Changes additional to those identified in the PDD were identified by Engineering Change Requests (ECR). These changes were reviewed, classified and analysed in accordance with the ICSA process. The results of all the analyses and related actions were kept in the ICSA register and on file.

All DRACAS records that were identified as having safety implications were referenced in the System Hazard Log. In cases where a DRACAS entry did not correspond to any of the existing System Hazard Log entries, it was subjected to safety analysis.

4.4.3 System Scoping and Conceptualisation

The system was depicted in the “System Architecture” document. The “System Architecture” describes all significant subsystems and internal and external interfaces of the system. The system architecture is presented in three levels of detail.

Starting with the highest level, depicting interfaces with objects outside the project scope and outside the railway, the second level provides a description of the main subsystems and their internal (internal to the system – scope of the project) relationship and finally providing the detail internal to the subsystem at the 3rd level of the description.

The system architecture was accompanied with an Objects & Interfaces database. All objects and their interfaces were described in this database.

Information about the changes to these interfaces throughout the project life (for each stage), detailing the changes was kept in this database. This information was then used to support ICSA and CSA sessions.

An example of the “System Architecture” diagram is on Figure 4-9 below.

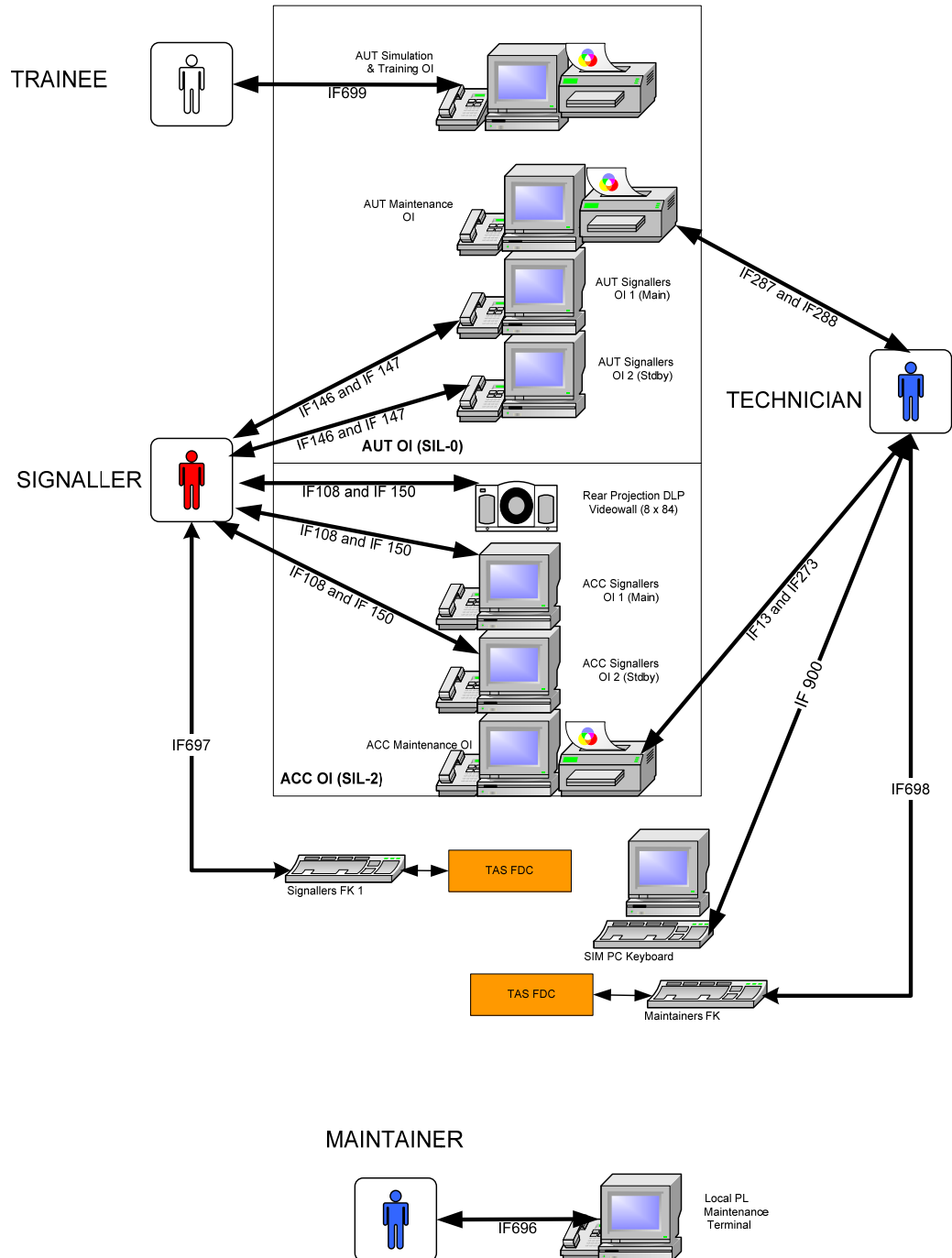


Figure 4-9: An example of the “System Architecture” diagram

4.4.4 Identification and Analysis of Hazards

Identification of Hazards was structured in the three parts (Lucic, 2004b):

- 1 Characterisation of Change and Identification of Safety Benefits;
- 2 Hazard Identification – Human Factors and Operational Issues;

- 3 Identification of Hazard Mitigations and Actions required which was undertaken in parallel with Hazard Identification.

Characterisation of Change and Identification of Safety Benefits

The purpose of this part of the study was to agree the scope, extent and purpose of the change in a form suitable for later stages of analysis and to identify the safety benefits of the change.

This was achieved by considering the following questions:

- 1 What is the change?
- 2 What is the rationale behind the way in which the changes are applied?
- 3 What is the intended function of the new equipment?
- 4 What is the environment in which the new equipment will be installed?
- 5 What does the new equipment interface to?
- 6 What non-equipment changes, if any are being made at the same time? (For instance, changes to maintenance regime or operational rules).
- 7 Which aspects of the equipment and its application are novel and which have been proven in service?
- 8 What are the safety benefits?

Identification of Hazards

A hazard is any possible state or behaviour of the signalling system or operator interaction with any inherent equipment within the system which might contribute to an incident. Actions of passengers and members of the public were not considered by CSA as these interfaces were outside of the project scope.

A brainstorm workshop was conducted to identify hazards, during which the changed functions, interfaces and equipment were considered. It was considered that the topic was well understood and that a structured brainstorm would be an efficient method of analysis.

The standard guide words, listed in Table 4-7 below, were applied to each interface affected by the change as described above. This provided structure to the hazard identification process.

The fact that a potential hazard was fully mitigated was not grounds for removing it. It was recorded in order to take full credit for the mitigation of the Hazard.

Guideword	Meaning	Sample Interpretations
NO or NOT	The complete negation of the intention	No execution, missing information, not ready, delay, earlier or later
MORE/EARLY	Quantitative increase	Parameters & items - too many time & range - too

Guideword	Meaning	Sample Interpretations
		high, too long (both singly and in combination)
LESS/LATE	Quantitative decrease	Parameters & items - too few time & range - too low, too short (both singly and in combination)
AS WELL AS	Qualitative increase	Parameters - extras, incorrect input, extra extension, different format actions - too many, too often, redundancy (in functions)
PART OF	Qualitative decrease	Incomplete input/operation, truncated, execute part of
REVERSE	The opposite of the intention	Opposite sign, feedback, inverse, negative parameters, go back
OTHER THAN / WRONG	Substitution of the intention	Intended input, intended operation, redirection of input, similar command, configuration control, wrong manual, wrong file, wrong value, unrequired act performed.

Table 4-7 : Hazard identification Standard Guide words

Mitigation of Remaining Hazards

The purpose of this part of the study was to identify any existing and planned, technical and procedural measures which mitigate the hazards remaining after the analysis performed above.

Following is an example of the outcome of the CSA workshop. For an interface: IF 13 (Diagnostics): From ACC Subsystem to Technician.

Characterisation of Change and Identification of Safety Benefits	
What is the change? (Confirm correctness of information in the Hazard Identification Study Briefing Document)	IF13.1. (P1): UK1 platform will have increased diagnostic. The maintainer gets a new alarms window which; • shows the alarms on the system as they happen, and displays a hierarchical version of the system which can be navigated • allows the maintainer to sort the alarms • allows the maintainer to suppress alarms from a specific part of the system, thus reducing the number of irrelevant alarms • notifies the maintainer when the alarm status is not available or reliable for a specific part of the system • notifies the maintainer when there is an alarm present in a specific part of the system • notifies the maintainer if the alarm is intermittent - i.e. comes and goes, thus reducing the number of irrelevant alarms displayed • suppresses alarms on equipment where a fault in the system makes the alarm status for that equipment unavailable or unreliable (Alarms are expected to latch. It is to do with ACC only no On-Line Diagnostic Terminal (i.e. SIM PC) (Action on G Lewis: Confirm that alarms for UK1 (Phase 1) are latching (as defined in the alarms specification) IF13.2. (P2): number of screens increased, screen configuration changed
What is the rationale behind the	DRACAS

way in which the changes are applied?	Different management of alarms needed
What is the intended function of the new function?	Improve alarms management
What is the environment in which the new equipment will be installed?	Same as before
What does the new equipment interface to?	Same as before
What non-equipment changes, if any are being made at the same time? (For instance, changes to maintenance regime or operational rules)	Maintenance regime of monitored equipment Possible change to operational rules should the equipment as implemented not function according to current Rule Book assumptions
Which aspects of the equipment and its application are novel and which have been proven in service?	Novel to the UK, used in Italy.
Safety benefits of change	For IF13.1. (P1): Improved maintenance gives you better system availability, which provides robust railway For IF13.2. (P2): Optimal visual presentation of information

Table 4-8: Characterisation of Change and Safety Benefits

And finally an example of the table of the records for the above interface, from the workshop:

Change Ref	Hazard	Cause	Mitigation	Action/Actionee	Guide word
IF13.1	No immediate hazard (Failure of diagnostics needs to be rectified as required)	Failure of diagnostics (no or wrong alarms)			No(info), part of
IF13.1	Unable to distinguish critical alarms	Too many alarms	Alarms level and thresholds should be set at appropriate level	J Bloke- Ensure that this is correct	Too early (report failures before they happen)
IF13.1	Not use the system properly, shift to unnecessary degraded mode of operation	Use of over restrictive controls	Design and testing of system to appropriate standards		Wrong (info)

Table 4-9: An example record from the CSA workshop.

4.4.5 Comparative Risk Assessment

All of the hazards were grouped in two categories:

1. The risks associated with the hazards that are understood and currently mitigated as standard practice; i.e. the risks are mitigated by following standards or other established authoritative good practice, and the project is actually following these

standards or other authoritative good practice. These hazards were not analysed further.

2. Novel hazards that originate from novel equipment, interfaces, or procedures, or from conventional equipment or procedures operating within the novel environment. These hazards were analysed further.

The risk associated with each novel hazard was categorised as follows:

BETTER: if the risk is assessed as significantly better than would be achieved with established conventional (like for like) means (in case of railway signalling for example with existing Solid State Interlocking, conventional UK signal heads etc);

OR

WORSE: if the risk is assessed as significantly worse than would be achieved with conventional (like for like) means;

OR

COMPARABLE: if the risk is assessed as neither Better nor Worse than would be achieved with conventional (like for like) means;

AND

MINOR: if there are other hazards associated with the scheme that have a risk at least an order of magnitude greater;

OR

MAJOR: if there are no other hazards associated with the scheme that have a risk at least an order of magnitude greater.

The risk associated with a hazard is considered acceptable only if it is:

MINOR and COMPARABLE or MINOR and BETTER or MAJOR and BETTER.

In general, the Hazard was declared as closed (managed to sufficiently safe level) when:

1. The risks associated with the hazards could be shown to be comparable with, or better than would be achieved with, a conventional scheme and no further reasonably practicable mitigation could be identified; or
2. In case of standard hazards or hazards originating from either the conventional systems already in use or standard procedures already applied on the railways, the closure of these hazards is justified through application of well established good practice, including Railway Group Standards and Network Rail Company Standards. These hazards were not further assessed.

Within the project timescales, options analysis concentrated on hazards classified as MAJOR, COMPARABLE which account for the majority of the risk. Each MAJOR, COMPARABLE hazard remaining at the end of the project phase was subjected to options analysis to underpin an argument that there are no reasonably practicable tactical options to reduce risk further.

A list of factors which act to drive risk up or down with respect to a conventional UK resignalling system was collected in support of a qualitative but rigorous argument that risk would not be reduced in the long-run by the strategic option of replacing the ACC with a conventional UK resignalling.

The ALARP argument rests in part on the conclusion that there are no tactical or reasonably practicable strategic options, which would reduce risk further.

As part of the options analysis, a list of performance metrics that would allow the project, to make a quantitative assessment of the risk associated with MAJOR, COMPARABLE hazards at a later stage was identified.

A recommendation to Network Rail to collect performance metrics was made.

4.4.6 Management Process

This section describes how project hazards will be identified, analysed and tracked to formal closure. Figure 4-10, below describes the Hazard Identification, Analysis and Management Process. Inputs to the process are:

1. Detailed description of interfaces extracted from a system Breakdown Structure. All interfaces were subjected to ICSA process as described above. To support the process it is necessary to understand the nature of interface, its performance limitations, operating environment, etc. All this information should be provided as part of interfaces description;
2. A detailed description of a change to the system subsequent to changes defined in the initial scope of the system change. This was done through Engineering Change Request process, where each change was recorded and subjected to ICSA process;
3. DRACAS process records were subjected to ICSA process as well. A review of the DRACAS records served dual purposes. Firstly, to assess safety impact of any changes to be introduced to the system and secondly to confirm correct functioning of identified and implemented mitigation measures.

Each change is subjected to ICSA, Category 2 and 3 changes are subjected to CSA. The results of the CSA are kept in the System Hazard Log, as well as references related to Category 1 interfaces. The System Hazard Log is used as a tool supporting the management process.

Each identified mitigation has been allocated to a responsible person on the project to implement. Proof of implementation was referenced/recorded in the System Hazard Log. These were subjected to a review by a team of suitably selected experts, to confirm satisfactory implementation of the mitigation measure. Upon agreement from the Hazard Forum (Lucic, 2002) the action to implement mitigation would be closed. Each hazard was subjected to an Options Analysis process as well, as described above. The deliverables of the process are:

1. **Initial Change Safety Analysis Records:** ICSA of an ECR was recorded in a spreadsheet and these records were kept under strict configuration control;
2. **Change Safety Analysis Briefing Document(s)** Change Safety Analysis Briefing Documents were produced to:
 - a. Provide practical details such as location of the meeting and agenda for the day;
 - b. Summarise the process to be followed for the session; for example the process to be followed for the identification of hazards;
 - c. Provide a technical description of the scope of the workshop.
3. **Change Safety Analysis Records:** The output of Change Safety Analysis activities were recorded in Change Safety Analysis Records. These records accurately document the process followed to clearly identify the agreed output.

The Change Safety Analysis records were reviewed and approved by the Hazard Forum.
4. **System Hazard Log** was the central repository for all system safety hazards identified for the project. The System Hazard Log was produced and maintained in accordance with the Project Hazard Log Management Procedure and according to the overall requirements of the Hazard Management Plan.

All system safety hazards identified across the project, by whatever means, were tracked to closure via the System Hazard Log. A key function of the System Hazard Log was to provide traceability from each hazard to all evidence used to justify its elimination or mitigation.

5. **System Hazard Reports** were issued at key milestones throughout the project, reporting on the status of all hazards within the System Hazard Log. These reports include a summary of the number of hazards in the System Hazard Log for each hazard classification (e.g. open, closed, mitigated etc).
6. **The System Hazard Log Report** contained the following information:
 - a. System Hazard Log Section, which describes the purpose of the System Hazard Log, its context in the history of the Project, the development of the System Hazard Log, its scope, use and underlying assumptions and constraints as well as a key to the fields in the Hazard Record Sheet and Hazard Summary List;
 - b. Journal of changes to the System Hazard Log;
 - c. Summary list of hazards and their status;
 - d. Hazard Record Sheets contain following information:
 - i. Information on the hazard: its unique reference number, description, and status. Information is also provided on the hazard's worst-case consequences should it occur, and the assessed frequency, probability and consequences of occurrence.
 - ii. A cross-reference is provided to the hazard's original source;
 - iii. Each cause of the hazard is uniquely numbered (with numbering derived from the hazard's number) and described;
 - iv. For each cause a listing of the actions to be taken and mitigations already in place is also provided;
 - v. Each action is uniquely numbered (with numbering derived from the relevant cause of the hazard) and described. Each action is allocated a nominated person to resolve the action, together with information supporting the action taken and/or mitigation proposed.
 - e. Directory of safety documents on the project.
 - f. List of consequences identified for all the hazards in the System Hazard Log.

7. **The System Hazard Log Implementation Audit Report** presented findings of the Project Hazard Log Implementation Audit (Lucic, 2003d).

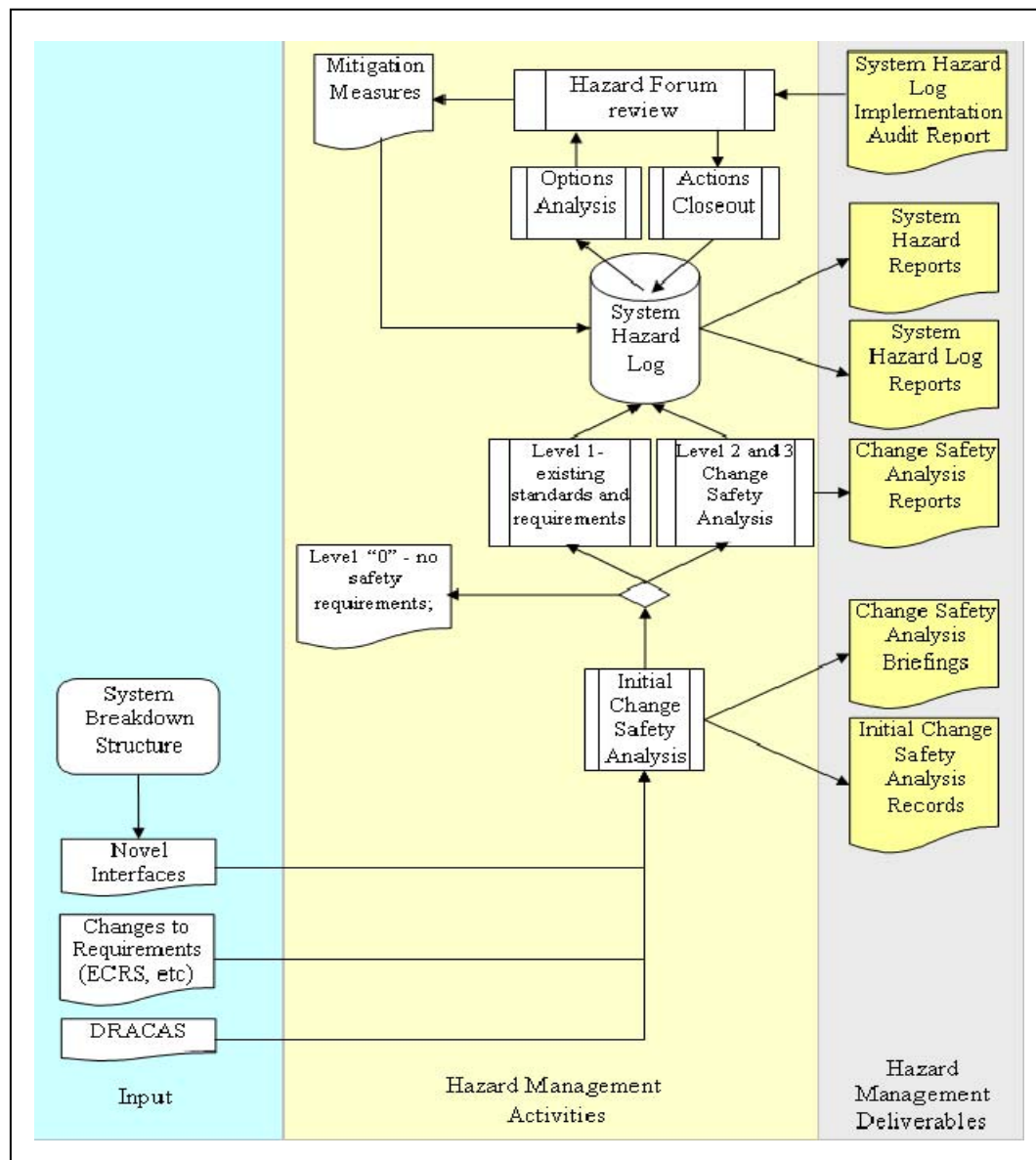


Figure 4-10: Management Process

4.5 Fourth Project: High Level Railway System Study - POLAND

4.5.1 Purpose and Scope of the Project

The Technical Assistance for Preparation of the Modernisation of Corridor II – Remaining Works project was aimed at enabling the Government of the Republic of Poland to make strategic decisions and financial commitments regarding the Modernisation of the Corridor II railway link. The geographical scope of the project includes the E20 section of the railway, Warszawa – Rzepin (excluding Poznań node), and the CE20 railway section, Łowicz – Skierniewice – Łuków.

The technical assistance project was realised in 5 stages:

Stage I: Feasibility Study - Cost Benefit analysis of three proposed options;

Stage II: Feasibility Study – Safety, Environment, Economic and Financial Analysis;

Stage III: Preliminary design;

Stage IV: Preparation of Application for EU funds;

Stage V: Elaboration of Tender documentation for contracts.

The author led the work at Stages I and II.

Three potential options were suggested:

Option 0: Basic construction work required to provide a minimum set of requirements with maximum limitations, resulting in a conventional railway line achieving the ERTMS compatibility at operational level only;

Option 1: Modernisation and upgrading of the infrastructure to Technical Standards for Interoperability of Conventional Rail System and AGC and AGTC standards for international corridors (maximum speed of 160km/h for passenger trains and 120km/h for freight trains). Therefore this option will mean introduction of ERTMS Level 2 railway line;

Option 2: Extension of option 1 to enable maximum speed 200 km/h, assuming use of tilting passenger trains, resulting in introduction of ERTMS Level 2 railway line as well.

For each Project Option, a number of different System Solutions is suggested.

As part of the activities within the first two stages of the project, a cost benefit analysis of the proposed three options and system solutions was carried out.

In order to achieve this it was necessary to identify relevant, high level, safety, RAM and environment protection requirements for each of the three proposed project options and to identify potential benefits that each proposed project option could bring.

In terms of compliance with EU standards and directives with regards to safety, the project had to, broadly, follow guidance provided in EN50126 and to be compliant with Control Command and Signalling (CCS) Technical Specification for Interoperability (TSI) Mandatory Specifications as follows:

1. Index 27: UNISIG SUBSET-091 Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2;
2. EN50126: Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). This standard is applicable to the whole of EU;
3. Other Specifications/Standards/Documents mandated by the TSI's;

and Informative Specifications as follows:

1. B43: 04E083 "Safety Requirements and Requirements to Safety Analysis for Interoperability for the Control-Command and Signalling Sub-System". Being a type "1", these specifications represent the current state of the work for the preparation of a mandatory specification still "reserved";
2. B44: 04E084 "Justification Report for the Safety Requirements and Requirements to Safety Analysis for Interoperability for the Control-Command and Signalling Sub-System". Being a type "2", these specifications give additional information, justifying the requirements in mandatory specifications and providing help for their application.

With regards to RAM there are documents produced in relation to ERTMS similar to safety which the projects have to comply with and refer to.

4.5.2 The Process for derivation of Safety & RAM requirements & Hazard Identification

Process-wise, the derivation of safety and RAM requirements was carried out in two steps, corresponding to the first two stages of the project, Stage I and Stage II:

Step 1: Identification of the high level safety, RAM and environment protection requirements for each of three proposed project options, as well as the benefits that each proposed project option, can bring to the system, for inclusion in the high level requirements baseline. At this stage of the project a very high level set of qualitative system requirements/policy statements, cross referenced to related standards (listed above) was identified, aimed at synchronisation of the project requirements with local Polish and ERTMS standards and high level requirements. For this step the requirements were defined in relation to overall system performance. The Polish railways do not have established safety targets for the railway network or railway lines, and therefore the project had to propose the approach to derivation of overall safety targets to Polish railway authorities (PKP) and the Safety Authorities.

Since the E20/CE20 railway line is part of TEN lines and the line is to be equipped with ERTMS Level 2 railway control system, it was logical to expect the safety performance to be at the same level as of other ERTMS fitted or planned lines in EU.

Consequently, the project made use of work done by UNISIG (RAMS target set at 10^{-9} dangerous failures for on board and track side ERTMS/ETCS equipment). Following the logic that safety performance of conventional signalling system must be same as that of ERTMS hence, the overall safety target for conventional system should be 10^{-9} , i.e. SIL4 (Safety Integrity Level).

Step 2: Derivation of more detailed requirements specification in support of tender documentation entailing apportionment of the identified/agreed overall system RAM and safety requirements to main system constituents. The RAM requirements were set at a different level of system decomposition to safety targets. At this stage a more detailed set of requirements was derived.

In order to do that, the project had to develop a high level functional system description inclusive of ERTMS and conventional system constituents and to identify interfaces for which the safety and RAM targets will be identified. Identification of the interfaces for which the project needs to define requirements, was dependant on the contracting/supply policy adopted by the project.

Using that system description, the HAZID study was organised to identify high level hazards which were mapped or cross referenced to existing list of CCS hazards as defined in B43: 04E083 and B44: 04E084. Other, non CCS parts of the railway system and related hazards were treated separately. This resulted in a complete list of railway system hazards and forms an initial hazard log for the project.

The outcome of Step 2 activities was:

1. A paper, for inclusion in tender documentation, stating:
 - a. References to relevant standards and directives;
 - b. System description used in support of the work;
 - c. List of RAMS requirements;
 - d. List of Assumptions, Dependences and Caveats;
 - e. List of identified system hazards.

2. A hazard log:
 - a. Hazard log in “paper” format for inclusion in tender documentation;
 - b. Hazard log database for handover to railway authorities and contractors.

4.5.3 System Scoping and Conceptualisation

In support of the first step (as defined above) a very high level of a system conceptualisation was developed (Lucic, 2006). It is possible to define 8 classes of different railway system constituents:

1. Controlled infrastructure;
2. Maintenance, Tools, equipment, machinery;
3. Trains;
4. Stations;
5. Stabling areas;
6. People (Procedures);
7. Railway neighbourhood;
8. Environmental factors.

Each of these can be broken into more detailed subclasses, as follows:

Class/Subclass	
1.	Controlled Infrastructure
1.1	Civil structures
1.2	Infrastructure based Communication Systems
1.3	Electrification
1.4	Level Crossings
1.5	Permanent way
1.6	Plant
1.7	Signalling (Conventional)
1.8	Signalling (ETCS trackside)
1.9	Infrastructure in general
2.	Maintenance, Tools, Equipment and Machinery
2.1	Maintenance Regime
2.2	Manual Tools
2.3	Instrumentation
2.4	Spares
2.5	Power Tools
2.6	Machinery(e.g. diggers)
3.	Trains
3.1	Braking Systems
3.2	Train Based Communication Systems
3.3	Doors
3.4	Running Gear
3.5	Traction systems
3.6	Train - Materials of Construction
3.7	Train Control (e.g. AWS, TPWS)

Class/Subclass	
3.8	Trainborne ETCS
3.9	Auxiliary Systems and Supply
3.10	Freight
3.11	Rail Based Machinery (e.g. ballast cleaners, tampers)
3.12	Material/Fuel
3.13	Other (i.e. technical or undetermined issues)
3.14	Corporate responsibility
4.	Stations
4.1	Escalators
4.2	Lifts
4.3	Non-public areas
4.4	Platform areas
4.5	Other station areas
4.6	All station areas
5.	Stabling Areas
5.1	Depots/workshops
5.2	Sidings
6.	People (Procedures)
6.1	Control room staff
6.2	Emergency response staff
6.3	Neighbours
6.4	Passengers
6.5	Station staff
6.6	Infrastructure maintainers
6.7	Train crew
6.8	Train maintainers
6.9	Operational Staff
6.10	All Staff
6.11	Corporate responsibility
6.12	Axle Counter operation specific procedures
6.13	Training
7.	Railway Neighbourhood
7.1	Construction
7.2	Hospitals
7.3	Housing
7.4	Industry/Factories
7.5	Roads
8.	Environmental Factors

Table 4-10: Railway system constituents classes and subclasses

In support of the Second step (as defined above) a more detailed, but still high level, system conceptualisation was done as presented on Figure 4-11 below.

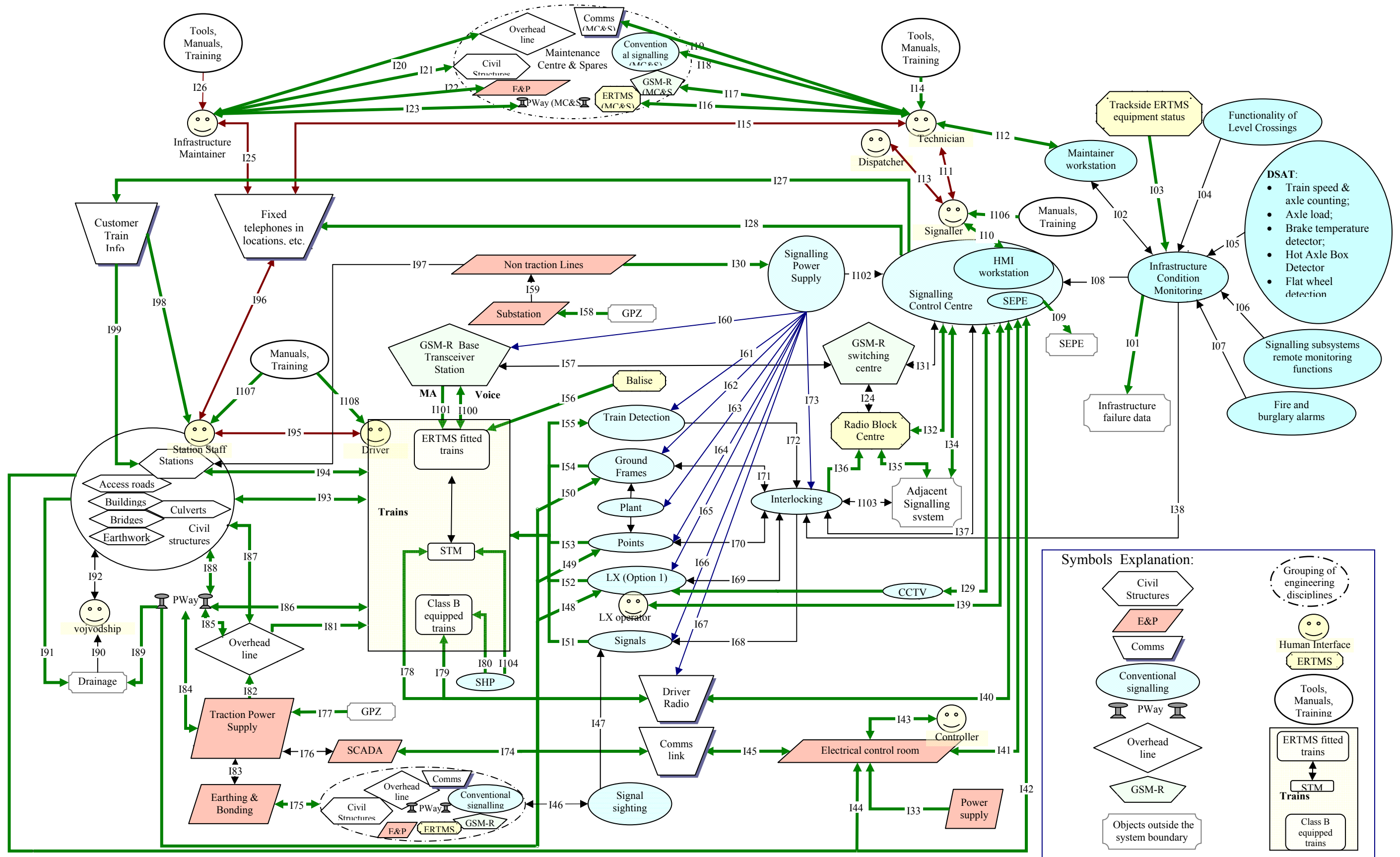


Figure 4-11: Railway System Model

A system boundary for which the analysis was to be done was identified and the relevant interfaces marked by different colours to denote different suppliers delivering different system constituents. All coloured interfaces are the boundary interfaces.

Each identified boundary interface, was reviewed to identify those interfaces (for each project option) that are not covered by existing standards, and for which it is necessary to identify the requirements and related potential hazard. Following table contains a sample of this information.

Requirements to be defined, hazards to be identified	Interface number	Interface between	
		Object	Object
Yes	I01	Infrastructure Condition Monitoring	Infrastructure failure data
No	I02	Maintainer workstation	Infrastructure Condition Monitoring
Yes	I03	Trackside ERTMS equipment status	Infrastructure Condition Monitoring
No	I04	Functionality of Level Crossings	Infrastructure Condition Monitoring

Table 4-11: An example of interfaces description

4.5.4 Derivation of High Level Safety Requirements

For each option, all of the classes listed in Table 4-10 above were reviewed to carry out identification of high level safety, RAM and environment protection requirements and benefits. The analysis was focused on identifying only those requirements that are not covered by existing Polish standards, for each class, during the review the basic stages of the system lifecycle were considered:

1. Installation;
2. Commissioning;
3. Operation (including maintenance);
4. Decommissioning.

The following table provides an example of the identified requirements not covered by existing standards for all project options, and the benefits.

Requirement Type/Benefiting area	Project option	Requirement/ Benefit description	Comment
Environment	Options 1 & 2	Noise management. Average level of noise, throughout the day, and during specific periods (day-time, night-time), should be kept within allowed limits. Possible approaches are: 1. Screens 2. Restricted use area procedure 3. Speed limit	Level of noise is likely to increase over time, if the infrastructure or rolling stock are not maintained correctly.
RAM	Options 1 & 2	Point heating needs to be adequate for speed and frequency of traffic	
Safety	Options 1 & 2	Project should consider/analyse EMI issues in consideration of supply of electricity to neighbours.	

Requirement Type/Benefiting area	Project option	Requirement/ Benefit description	Comment
Environment	Option 1	Minimising risk of ground and surface water contamination by hazardous goods in regular operation.	
RAM	Options 1 & 2	Improved technical condition of structures.	
Commercial	Option 2	Adjustment of whole line for 200km/h for option 2, leads to significantly reduced travel time	Only applies to E20 - not CE20.
Safety	Options 1 & 2	Improved safety at road/rail crossings	

Table 4-12: Example of high level safety requirements

4.5.5 Identification of Hazards

This analysis has been based on the above system description. In support of this analysis the author prepared a list of 32 high level railway hazards. A sample from the list of hazards given in the Table 4-13 below was reviewed by the team of experts to establish its completeness.

Ref.	Hazard name	Hazard Description/Scope
CH1.	Abnormal deceleration	The hazard “Abnormal deceleration” includes only those instances of a train’s slowing sharply when not actually as a part of a derailment or collision scenario. Includes all 3 groups, Passengers, Neighbours and Workers.
CH2.	Contaminated water and/or land and/or air	The Hazard for Contaminated Water and/or Land has been defined as the release of harmful substances likely to cause contamination of the environment. This allows the consideration of detection, mitigation and remediation barriers in the consequence domain. The release of toxic gases likely to cause harm to workers or neighbours has also been considered under this core hazard. This Core Hazard considers harm to workers or neighbours as a result of coming into contact with land, water or air contaminated with harmful substances, rather than coming into contact with the harmful substances themselves - although the toxicology is similar, the frequency and dispersion will differ. Includes Neighbours and Workers.
CH3.	Crossing running railway at level crossing	Includes all situations in which a user (i.e. a Neighbour) is present on a level crossing without the intended degree of protection from trains. This may arise from intentional or inadvertent misuse of the crossing by the Neighbour as well as from failures and errors in railway equipment and procedures. The definition excludes situations in which harm may arise when using a level crossing as intended, for example if a user falls and injures themselves on a crossing but is still able to cross within the design time limit. The hazard excludes incidents at level crossings resulting from suicide or attempted suicide - these are assumed to be covered under Abnormal or Criminal Behaviour The hazard is limited to Neighbour hazards and thus does not consider hazards at worker crossings provided within stations, depots, sidings etc. Unauthorised Neighbour use of such crossings should be regarded as Abnormal or Criminal Behaviour, being a form of trespass. (Unauthorised passenger use is covered in Hazard Inappropriate Separation between Running Railway and people.)
CH4.	Electro-Magnetic Interference (EMI) caused to by railway operations	EMI Caused by Railway Operations to Businesses, General Public, Adjacent Buildings, Hospitals, has been developed to include those situations where EMI from the infrastructure or rolling stock could affect the safety of neighbours directly. This hazard does not include EMI caused by infrastructure or rolling stock to signalling and track circuits, or interference between the rolling stock and infrastructure. Such

Ref.	Hazard name	Hazard Description/Scope
		interference could be considered part of the causes for other hazards.
CH5.	Inappropriate separation between trains	The hazard Inappropriate separation between trains includes the scenarios in which the determined separation between trains, normally provided by the signalling system, has broken down. This hazard is defined such that there is no interface between it and the “Loss of Balance” hazard. Includes all 3 groups, Passengers, Neighbours and Workers.
CH6.	Inappropriate working methods/environment	The scope of this hazard was defined to include most “occupational” accidents where typically a single worker is affected. Also included is the case of crane loads and other mechanical equipment fouling trains passing nearby as this was always due to operator error.

Table 4-13: High level railway hazards

Each identified interface was reviewed against a list of hazards and related to applicable hazards as in a Table 4-14 below.

Related interfaces (interface reference: from “subsystem” to “subsystem”)	Related core hazards
I088: Civil Structures - PWay	CH27. Unsound/unsecured structures; CH15. Incompatibility of train and structure gauge;
I089: PWay - Drainage	CH27. Unsound/unsecured structures; CH03. Contaminated water and/or land and/or air; CH18. Loss of train guidance (derailment); CH30. Loss or degraded train detection
I084: PWay - Traction Power Supply	CH06. Electro-Magnetic Interference (EMI) caused to by railway operations; CH13. Inappropriate separation between uninsulated live conductors & people;
I085: PWay - Overhead line	CH13. Inappropriate separation between uninsulated live conductors & people; CH15. Incompatibility of train and structure gauge;
I086: PWay - Trains	CH09. Impact from railway construction/maintenance works; CH20. Objects/Animals on the line; CH18. Loss of train guidance (derailment); CH02. Abnormal deceleration; CH31. Loss of adhesion (abnormal acceleration/deceleration)

Table 4-14: Initial System Hazard Log sample (Core Hazards referenced to originating system interfaces)

The result of this study established a hazard log for the project and was used to evaluate different project options and choose the most appropriate one for implementation within the funding scope and proposal for modernisation of the Corridor II.

4.6 Chapter Conclusions

In this chapter the author depicted the experience and findings related to an application of some of the existing methodologies on 4 very different railway projects as well as the background to and results of the implementation of several innovative methodologies that the author developed whilst working on these projects. A more detailed critique of the methods detailed here is provided in the next chapter.

*The safest road to hell is the gradual one - the gentle slope, soft
underfoot, without sudden turnings, without milestones, without signposts*
- C.S.Lewis

CHAPTER 5: CRITIQUE OF CURRENT THINKING, AVAILABLE TOOLS AND PRACTICE A RESEARCH AGENDA

5.1 Chapter Introduction

The requirements for the new system based framework for system safety analysis and management are identified and outlined in this chapter. Based on that existing tools and methodologies have been assessed for compliance with requirements and a research agenda set out.

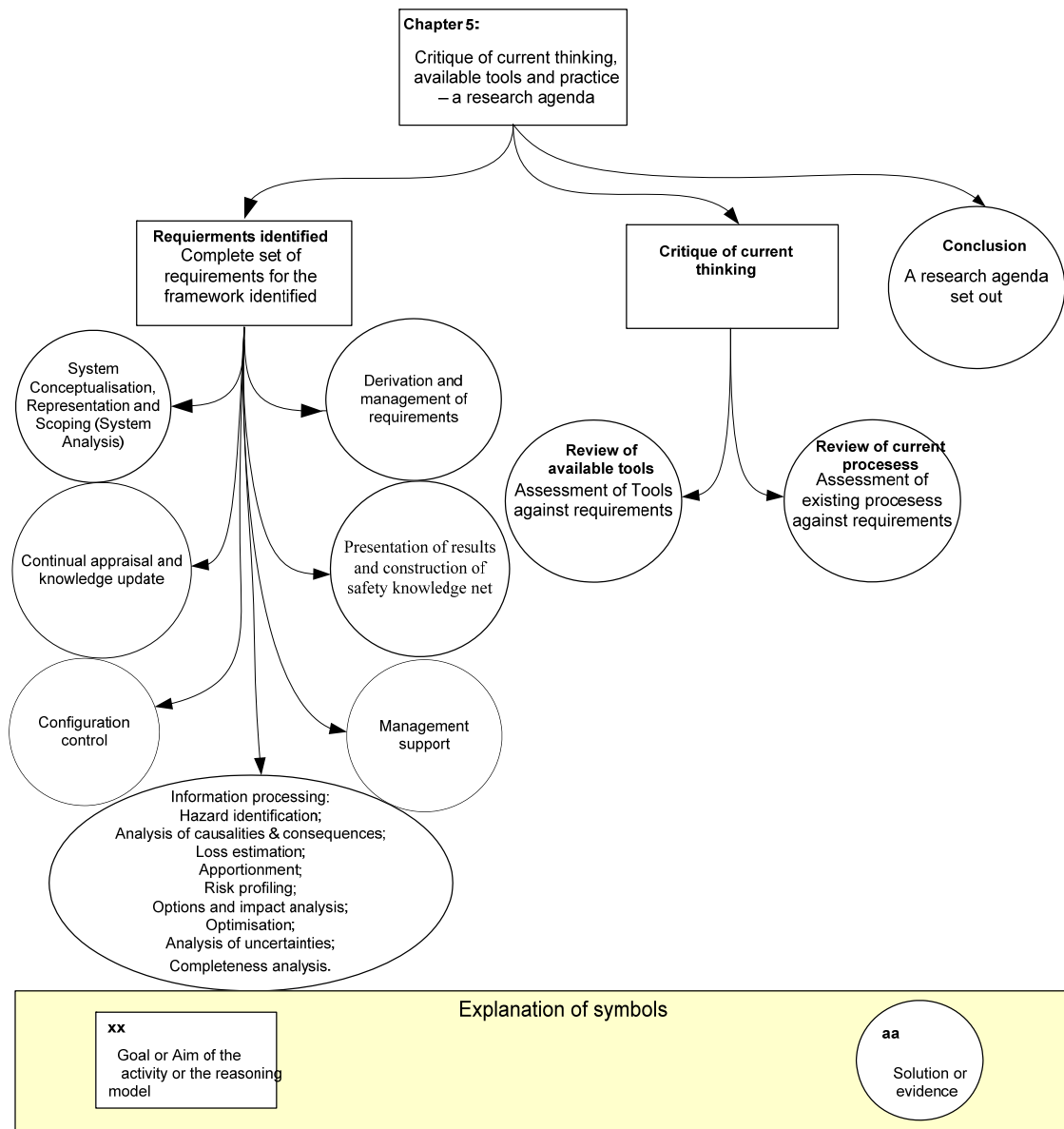


Figure 5-1: Structure of chapter 5

5.2 Summary of Requirements for new framework

Following generic safety risk analysis and management stages applicable to any system (or undertaking) have been identified as part of this research:

1. System Conceptualisation, Representation and Scoping (System Analysis). This stage of the analysis is often omitted from safety literature and standards. This preparatory phase is necessary in order to provide a structured framework and systematic approach for the hazard identification and risk assessment and support a holistic approach to the analysis. Some form of system description model, for example state transition model or sequence and collaboration diagram should be used as the basis for hazard identification, as the hazards resulting from each system interface, process or interaction can be elicited. The novel approach, developed as part of the research, to system conceptualisation in support of safety analysis is discussed later in the thesis;
2. Information processing can be further structured in a number of activities:
 - a. Hazard identification. The purpose of this stage of the process is to identify dangerous states associated with the system and its operation as detailed earlier (BS EN 50129, 2003), (CENELEC 1998), (CENELEC 2003), (BS EN 50126: 1999), (BS EN 50129: 2003), (BS EN 61508: 2003), (RSSB, 2007). Although hazards and identification of hazards is at heart of any safety analysis, not much work has been done defining the properties of hazards. A formal definition of a hazard and the properties of the hazard has been developed and is presented later in this thesis. Also in combination with the novel approach to system conceptualisation, a formal process supporting hazard identification has been developed;
 - b. Analysis of causalities and consequences. The objective of the causal analysis is to determine the relevant factors, which act singularly or in combination, in the realisation of a hazard. The objective of the consequence analysis is to identify the scenarios arising from a hazard to consequences and the consequences themselves (BS EN 50129, 2003), (CENELEC 1998), (CENELEC 2003), (BS EN 50126: 1999), (BS EN 50129: 2003), (BS EN 61508: 2003), (RSSB, 2007). As part of the hazard identification a structure is provided in support of the cause and consequence analysis;
 - c. Loss estimation, is about the assessment of the magnitude of the detrimental impact associated with consequences (BS EN 50129, 2003), (CENELEC 1998), (CENELEC 2003), (BS EN 50126: 1999), (BS EN 50129: 2003), (BS EN 61508: 2003), (RSSB, 2007);

- d. Estimation and apportionment of the safety risk to the source causes and failures of preventative measures is important to enable identification of the most critical constituents of the system and focus the improvement efforts in the most fruitful areas of the system. Some work has been done in this area (Saltelli, 2002). The author developed a novel, formal methodology to perform the apportionment of risk within the cause-consequence modelling environment (Lucic, 2004a). This novel methodology is discussed further later in the thesis;
- e. Risk profiling. Risk profile is a multi dimensional presentation of forecasts for future accidents for a system. Additional dimensions introduced, may be time, space, or some other important variable parameters. A novel approach to risk profiling has been developed including supporting tools (Lucic, 2003a), (Lucic, 2004a) and is discussed later in the thesis;
- f. Identification of different solutions and mitigation measures (options and impact analysis) is a prerequisite to any claim that the safety risks of the system are As Low As Reasonably Practicable. This involves identification of any additional potential mitigation measures or different options to a system solution or implementation that could further reduce the safety risk (Health and Safety Executive, 2009), (RSSB, 2007). A structured approach to conceptualisation and hazard identification developed as part of the research supports this stage of the analysis in a novel way, as discussed later in this thesis;
- g. Optimisation of the system and selection of the most gainful options and mitigations is carried out to ensure the safest possible solution (Health and Safety Executive, 2009), (RSSB, 2007). This can be done using a quantitative or qualitative methodology. Both methodologies are further developed and discussed in this thesis;
- h. Analysis of uncertainties includes assessment of a level of imprecision of numerical data or understanding of the system composition and behaviour and appraisal of the potential impact of this uncertainty on the analysis;
- i. Completeness analysis is necessary to confirm that none of the possible system's states or configurations or potential scenarios is overlooked. As part of a novel system conceptualisation approach, a framework for completeness assessment and assurance has been development;

3. Derivation and management of requirements. Outputs of the analysis process are identified mitigations or options to be implemented in the system, or identified limits of safe operational envelope for the system. These need to be expressed as requirements and managed throughout the life of the systems. Confirmation that the requirements are implemented is usually obtained through the verification and validation process (Blanchard and Fabrycky, 1998). Derivation and management of safety requirements is important as one of the options to confirm final safety performance of the system is through verification and validation of safety requirements;
4. Presentation of results and construction of safety knowledge net. Throughout the analysis, knowledge about the system is collected in a number of cycles (preliminary analysis, design analysis, system change analysis, etc.) corresponding to the principal engineering safety management activities, mentioned earlier. As development of the system is progressing, more knowledge is gathered and merged with already processed information. This accumulated knowledge is then manipulated to generate the forecasts for the system's safety performance.

Often the complexity of analysed system dictates that the problem domain is broken into digestible chunks. Prior to analysis, the system is broken into subsystems, elements of the big puzzle that can be comprehended. The analytical work is performed on these palatable chunks to produce constituents of the concluding result. Finally, using the elements of the answer, the freshly formed cells of knowledge are merged into a net defining the new understanding of the analysed system. This approach enables easy update of understanding of the system with new information.

One of major aims of risk assessment is to ascertain the safety performance of the system and determine if it is satisfactory. Decision about the adequacy of the safety performance of the system is based on knowledge gathered during the analysis. Structuring of safety arguments into knowledge net enables systematic review of gathered knowledge. Furthermore, it is necessary to create different views on the information, a person responsible for implementation of a mitigation measure may not need the same information as the tester of the same mitigation, or maintainer of the subsystem that provides the mitigation. It is, therefore necessary to identify these different view points on the knowledge net, and make it possible to create the required output (Kelly and Weaver, 2004),

(Kelly, 2001). A novel process developed as part of the research and presented latter in this thesis, extends beyond the existing knowledge management and presentation methods brought by the Goal Structuring Notation (Kelly and Weaver, 2004), (Kelly, 2001);

5. Management support. Any safety management process, must be capable of supporting management and recording any activities related to the analysis, implementation of mitigations, options and requirements, verification and validation and finally testing (RSSB, 2007), (Hessami, 1999b). Processes supporting the management needs, are embedded in the novel process developed as part of the research and presented latter in this thesis;
6. Configuration control. All the time configuration control of all the information must be kept, all our assumptions must be documented and the work must be transparent and understandable to others (RSSB, 2007);
7. Continual appraisal and knowledge update. As the system is being developed, used and decommissioned, it is necessary to monitor the safety performance of the system, and to update the knowledge base as required. It is only if the knowledge about the system is up to date that the safety management of the system can be effective (RSSB, 2007). A novel process developed as part of the research and presented later in this thesis also facilitates appraisal and knowledge update and management.

Any new framework for analysis and management of system safety needs to include all of the above stages into a holistic methodology.

In addition to above the methodology must be able to cope with the added complexities of staged project implementation, intricate supply chains and delivery organisations pertinent to so many contemporary projects.

5.3 Critique of current thinking

The work done under the general umbrella of safety management is in fact knowledge elicitation and gathering and subsequent knowledge and corrective action management.

Information is collected, presented in a hopefully easy to understand form, more information is collected and merged with already processed information, accumulated knowledge is manipulated and the arguments in support of derivation of a safety case generated.

Once the initial phase of the project is completed the stakeholder should continue with the maintenance of the knowledge base and management of corrective actions until decommissioning.

All the time configuration control of all the information must be kept, all the assumptions must be documented and the work must be transparent and understandable to others.

From the start to the end of the process the complexity of modern systems (engineering and organisational) necessitates the need to break the problem area into digestible chunks. Prior to analysis, the system is broken into subsystems, elements of the big puzzle that can be comprehended. The analytical work is performed on these palatable chunks to produce constituents of the concluding result.

Finally, using the elements of the answer, the freshly formed cells of knowledge, “freshly trained neurons”, are merged into a large “brain” containing new understanding of the analysed/managed system.

Development of models in support of this process has the potential to greatly improve the development of conclusions underpinning safety arguments. The individual projects can be supported by models as follows:

1. Models are an instrument that enables better understanding of a system being implemented/maintained;
2. Development of the comprehensive set of safety arguments would benefit from a good set of models describing the system and supporting the risk assessment;
3. Safety risk based, quantified comparison of effectiveness of different solutions in support of options analysis;
4. Quantified estimation of safety risk introduced to the system by implementation of new technology and processes, in support of ALARP argument;
5. Model logical structures can be used in support of systems analysis enhancing the understanding of the technological and procedural solution for the project.

Use of modelling on a project is not a prerequisite for a successful conclusion of the undertaking, but it supports efficient, concise and structured knowledge gathering, structuring of the argument and enables quantified support to the decision-making process.

However, modelling of any kind is expensive and the Systems Safety Analysis and

Management budget should be carefully balanced to enable completion of all steps of the process. If a decision has been made to develop models in support of the project, the complexity brought about by increased sophistication in modelling should be balanced against the difficulties in understanding by experts and the likelihood of introducing systematic errors. As already mention earlier in “Objectives and Aim of the Research“, a number of generic activities of safety risk analysis and management process have been identified.

The table below provides an overview of these activities in relation to methodologies reviewed in the previous sections of the thesis. Although all of the above mentioned methodologies are useful on their own, none of these covers the complete set of activities required to support the system safety risk analysis and management process, as depicted above.

At the moment an integrated framework for the system safety risk analysis and management does not exist. Currently, the most advanced and structured process for Systems Safety Analysis and Management is presented by the 7 Stage Process and its extension Risk and Opportunity paradigm.

The ISAE8 (a tool set used for development of parametric models described later in the thesis) is a very comprehensive as it brings together following facilities:

1. Hazard log;
2. Risk modelling environment;
3. Reporting.

However most of the other generic activities are not part of the process or the tool. Most of the methodologies listed above are not particularly user friendly and are very difficult and expensive to implement and maintain on the large scale project. As the complexity of the analysed system increases the models produced using the existing techniques tend to increase in complexity at even faster rate, resulting in extremely complex models, that are difficult to validate and test, and finally, due to their complexity, end up not being used in support of the projects.

Although some of the models are capable of supporting the analysis of temporal and spatial aspects of the systems safety risk, the results are snapshots in time and do not land themselves to profiling of risk. Furthermore apart from the Weighted Factors Analysis none of the methodologies are capable of taking into account effects of both detrimental and beneficial facets of the systems behaviour to the safety of the systems.

Methodologies \ Activities	System Description Models	System Dynamics	Failure Mode and Effects Analysis	Theories of Probability	Monte Carlo Simulation Models	Theory of Evidence	Reliability Block Diagrams and Network Models	Fault Trees – Event Trees	Markov Models	Petri Nets	Theory of Fuzzy Sets	Weighted factors Analysis	Advanced Cause Consequence Models	Parametric Advanced Cause Consequence Models
System analysis/conceptualisation	✓	n/a	n/a	n/a	n/a	n/a	✓	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Hazard identification	✓	n/a	n/a	n/a	n/a	n/a	✓	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Analysis of causalities	n/a	n/a	✓	✓	n/a	n/a	✓	✓	✓	✓	✓	✓	✓	✓
Analysis of consequences	n/a	n/a	✓	✓	n/a	n/a	✓	✓	✓	✓	✓	✓	✓	✓
Loss estimation	n/a	✓	✓	✓	✓	n/a	n/a	n/a	n/a	n/a	n/a	n/a	✓	✓
Apportionment	n/a	n/a	✓	✓	n/a	n/a	n/a	✓	n/a	n/a	n/a	n/a	✓	✓
Options analysis	n/a	n/a	n/a	n/a	n/a	n/a	✓	✓	✓	✓	✓	✓	✓	✓
Impact assessment	n/a	n/a	✓	✓	✓	n/a	n/a	✓	✓	✓	✓	n/a	✓	✓
Risk Profiling	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	✓
Optimisation	n/a	n/a	n/a	✓	✓	n/a	n/a	✓	✓	✓	✓	n/a	✓	✓
Construction of safety arguments network	n/a	n/a	n/a	n/a	n/a	✓	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Requirements derivation	n/a	n/a	n/a	n/a	n/a	n/a	n/a	✓	✓	✓	✓	✓	✓	✓
Configuration control	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Management support	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Continual appraisal and knowledge update	n/a	n/a	n/a	✓	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Reporting.	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Table 5-1: Comparison of facilities provided by different methodologies.

Development of the methodology supporting the generic activities of safety risk analysis and management process for any system would bring benefits to the industry. Moreover, since the current practice in the UK is that demonstration of compliance with the ALARP principle is structured in the form of a Safety Case, the process needs to support the development of the Safety Case.

5.4 Chapter Conclusions

In this chapter the author identified and outlined the requirements for the new system based framework for system safety analysis and management. Furthermore, using the framework requirements as the baseline, the author analysed the existing methodologies, drawing on the experience depicted in Chapter 4, and summarised the critique of current thinking in this chapter.

Our plans miscarry because they have no aim. When a man does not know which harbour he is making for, no wind is the right wind - *Seneca*

CHAPTER 6: A NEW SYSTEMS BASED APPROACH TO SYSTEM SAFETY RISK ANALYSIS AND MANAGEMENT

6.1 Chapter introduction

The findings of the initial part of the research, development of a new system based approach to safety risk analysis and management theory is discussed here.

Before one can begin defining the process for information gathering, conceptualisation and representation (System Analysis) in relation to safety risk analysis, assessment and management, it is necessary to define the properties of the hazard, as an element of the risk, and outline the requirements and structure of the Safety Case as a final deliverable of all the analysis.

Hence the first two sections of the chapter are presenting the research findings regarding this subject.

Discussion about the development of the new framework follows in rest of the sections in this chapter. Integration of the novel methodologies discussed in Chapter 4 and some of the existing methods outlined in Chapters 3 and 4, into a new framework is presented and discussed.

Figure 6-1 below provides an overview of the structure of this chapter, presents the lines of reasoning followed in support of the development and indicates which parts of the process (or which methodology) is newly developed or is a new application of existing one.

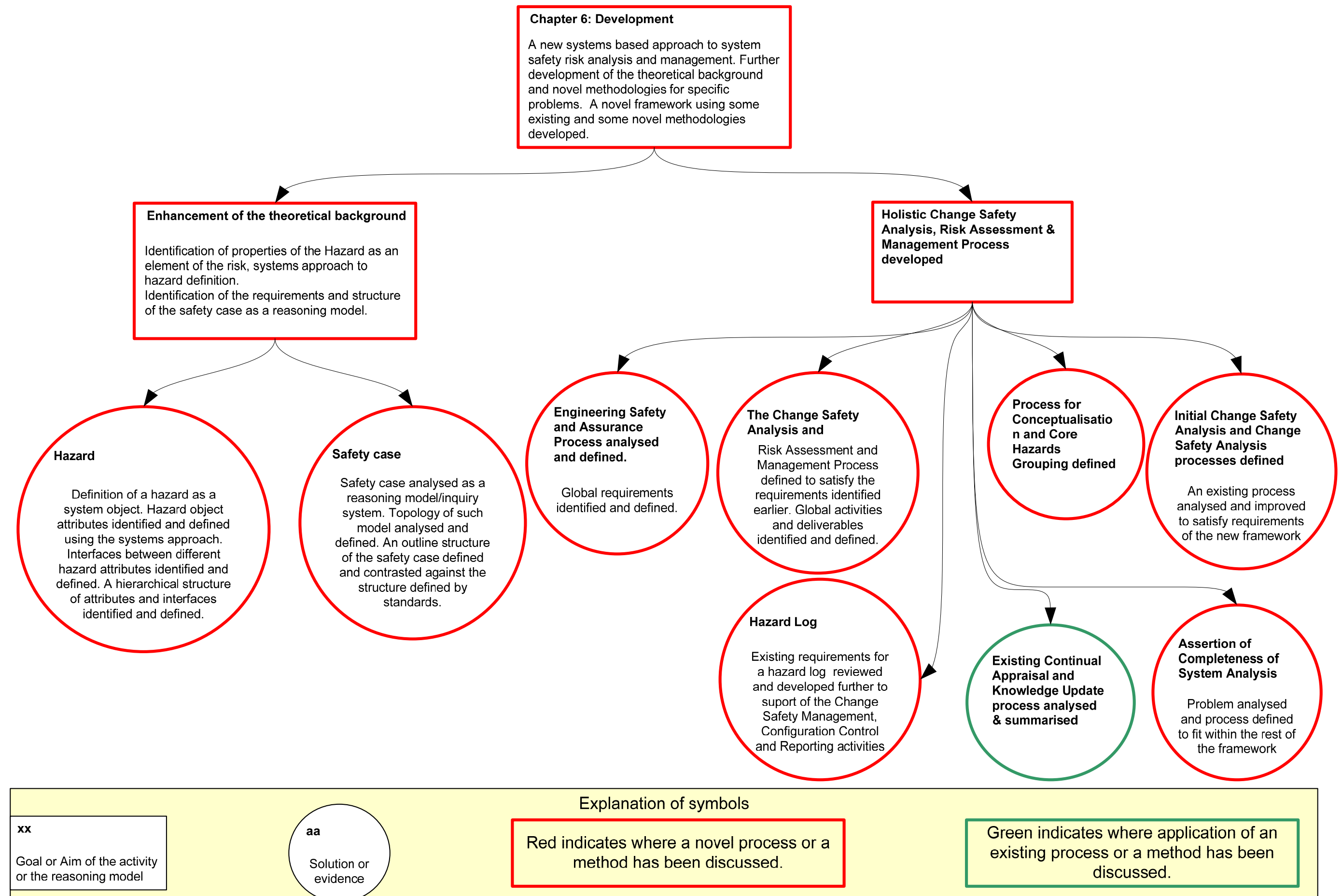


Figure 6-1: Structure of chapter 6 and the argument in support of the claim that a newly developed process is sound and complete

6.2 The Hazard

A hazard is characterised by its potential to cause an accident, as already discussed earlier. However, the real picture is more complex.

Different sets of attributes define different objects that make up each hazard, as well as the relationships between each individual hazard and all the different hazards that are parts of the entirety of “safety performance” as an emergent property of any system under observation.

Furthermore, each of these sets of attributes and their internal and external relationships is characterised by its own properties.

We will refer to this entirety as the “hazard universe”.

It is possible to identify at least two different (but related) view points on the problem domain:

1. Analytical or System Safety point of view;
2. Management point of view.

Both of these will be analysed separately and a unified, holistic relational data structure depicting the “hazard universe” will be proposed.

Analysing the hazard, from a systems safety point of view, it is possible to define the “hazard universe” as a hierarchical net, consisting of a number of different objects, interacting to define the Safety Performance as an emerging property.

If we analyse the hazard from a systems point of view, it is possible to distinguish between three sets of attributes related to each hazard:

1. Attributes related to the origin of the hazard, causality of the hazard (spatial and temporal);
2. Attributes related to the evolution of the hazard, post hazard horizon, (spatial and temporal) into a consequence or set of consequences, defining the frequency of the consequences;
3. Spatial and temporal attributes related to the consequences, defining the nature of the consequences and subsequent loss.

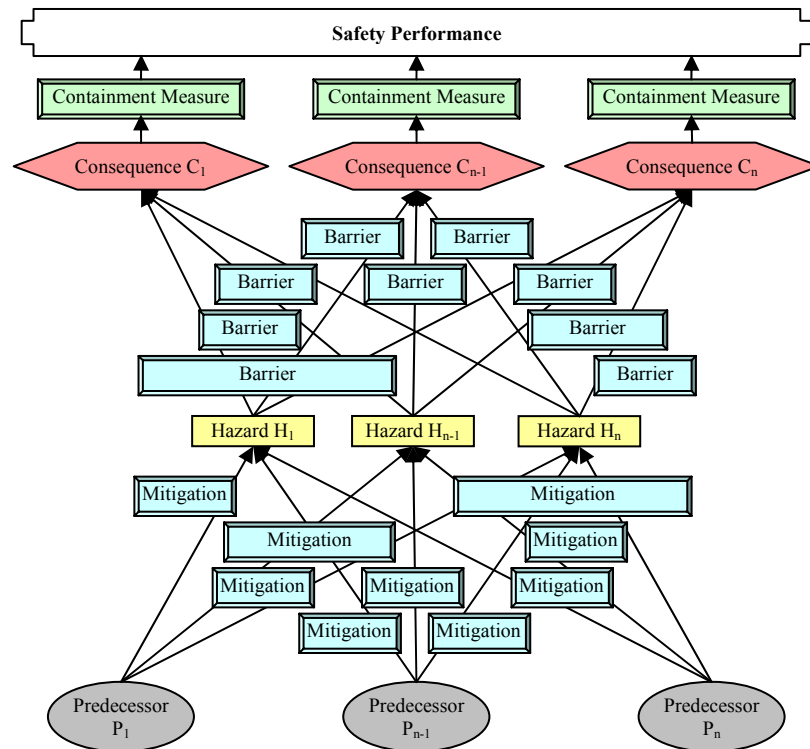


Figure 6-2: “Hazard Universe”

Interactions of these three sets of attributes define the attributes of the hazard itself.

The collective effect of interactions between different hazards (in fact these are interactions between attributes of individual hazards) could be seen as emerging properties of the “hazard universe”, where the “hazard universe” is treated as a system:

1. Potential detriment, risk, which the hazard can initiate (as an emerging property defined by combined spatial and temporal effects of attributes related to the origin of the hazard, attributes related to the evolution of the hazard into a consequence or set of consequences, consequences themselves and of any containments of consequences);
2. The spatial and temporal nature of the hazard itself (as an emerging property defined by the combined spatial and temporal effects of attributes related to the origin of the hazard).

Attributes related to the origin of the hazard could be treated as constituents of the “hazard universe” system, which interacting together define the causal properties of each of the hazards, and of the “hazard universe”, with their own properties:

1. The cause or causes (predecessor(s)) of the hazard;
 - a. Spatial properties, location of the predecessor(s) to the hazard;
 - b. Temporal nature of the predecessor(s) to the hazard;
 - c. Nature of relationship between different causes;

- d. Potential relationship between causes and protection/defence measures (causes instigating failures of protection/defence measures);
 - e. In case that there is more than one predecessor, a measure of contribution of the predecessor to the hazard;
2. The mitigations of causes. The attributes of mitigations are:
- a. Nature of relationship between the cause and the mitigation;
 - b. Nature of relationship between different mitigations;
 - c. A measure of reduction of the detrimental effect of the cause or contribution to the hazard.

Attributes related to the evolution of the hazard into a consequence, “post hazard horizon”, could be treated as constituents of the “hazard universe” system, which interacting together define the consequences of each of the hazards, and of the “hazard universe”, with their own properties:

- 1. The barriers to the hazard, reducing the effect of the hazard;
 - a. Spatial properties, location of the barrier(s) to the hazard;
 - b. Temporal nature of the barrier(s) to the hazard;
 - c. Nature of relationship between different barriers;
 - d. In case that there is more than one barrier, a measure of reduction of the detrimental effect of hazard;
 - e. Nature of relationship between the causal domain of the hazard and the barriers;
 - f. Nature of relationship between different barriers.
- 2. Attributes related to the progression of consequences and effect of the containment measures, “post consequence horizon”, could be treated as constituents of the “hazard universe” system, which interacting together characterize the safety performance of the system under observation and its “hazard” universe:
 - a. Frequency or probability of consequence occurrence;
 - b. Temporal nature of the consequence;
 - c. Spatial properties, location of the consequence;

- d. Nature of subsequent loss;
 - e. Exposed party (who will suffer the loss);
 - f. Potential for direct consequences causing further subsequent consequences;
 - g. Nature of relationship between different consequences;
3. And finally, containment measures:
- a. Spatial properties, location of the containment measure(s);
 - b. Temporal nature of the containment measure(s);
 - c. Nature of relationship between different containment measures;
 - d. A measure of reduction of the loss;
 - e. Nature of relationship between different containment measures.

In support of safety management process it is usual to create a log of all hazards on the project and track implementation of any defence/protection measures using this log.

The author will talk about the use of the Hazard Log and its place in the management processes later. However for purpose of this analysis the author identified that additional information is required. A distinction should be made between the attributes of the “hazard universe” from a systems safety point of view, and information needed in support of safety management process.

It is possible to classify these information items into two categories:

- 1. Support to a comprehensive audit trail;
 - a. Source of identification of each object of the “hazard universe”;
 - b. Any documents that are relevant/related to the object;
 - c. In case of actions, information supporting closure, confirmation that the defence/protection measure is in place and working;
 - d. Journal, a record of all changes to the hazard log;
 - e. Configuration control information;
- 2. Management of actions to implement or confirm implementation of identified defence/protection measures
 - a. Hazard:
 - i. Status of the hazard:

- Hazard is **OPEN** if risk emerging from the hazard is unacceptable and defence/protection measures introduced or identified are not sufficient to mitigate the risk to an acceptable level;
 - Hazard is **CONDITIONALLY CLOSED** if existing and new identified (but not yet implemented) defence/protection measures are sufficient to mitigate the risk to an acceptable level;
 - Hazard is **CLOSED-Mitigated** if existing defence/protection measures are sufficient to mitigate the risk to an acceptable level. However it does not mean that this hazard is forgotten, as discussed earlier. We will discuss the Safety Management process later in more detail;
 - Hazard is **CLOSED-Eliminated** if hazard is completely eliminated, for example by design. Again it does not mean that this hazard is forgotten and we will discuss the Safety Management process later in more detail;
 - Other statuses are possible (for example **TRANSFERRED** when responsibility for safety management of the hazard is transferred to some other project or party or **CANCELLED** if after initial analysis it is confirmed that what was initially hazard actually does not exist) but first four are the most important;
- ii. Disposition statement is clarification of the hazard status and record of any changes to the hazard.
- b. Defence/Protection measures:
- i. Action Description provides detail about the action to implement the defence/protection measures;
 - ii. Action Status
 - Action is **OPEN** if it is not implemented;
 - Action is **CONDITIONALLY CLOSED** if it is certain that the action will be implemented;
 - Action is **CLOSED** if related defence/protection measure is implemented;
 - Similar to hazard, other statuses are possible (for example **TRANSFERRED** or **CANCELLED**) but unlike hazard, once the action

is transferred or cancelled it is usually kept only as a record of earlier activities;

- iii. Actionee is responsible to implement the defence/protection measure;
- iv. Actionee response is the status report regarding the implementation of the action and Action implementation deadline date is providing a timescale for implementation of the action;
- v. References to relevant safety requirements provides link to the system requirements set. A subset of defence/protection measures will refer to “things” that exist already and some to those that are needed to make the system acceptably safe. These defence/protection measures should be transformed into requirements.

Following diagram (Figure 6-3) depicts the above described attributes (coloured yellow), information items (blue for audit trial related items and white for management of actions related items) and their relationship.

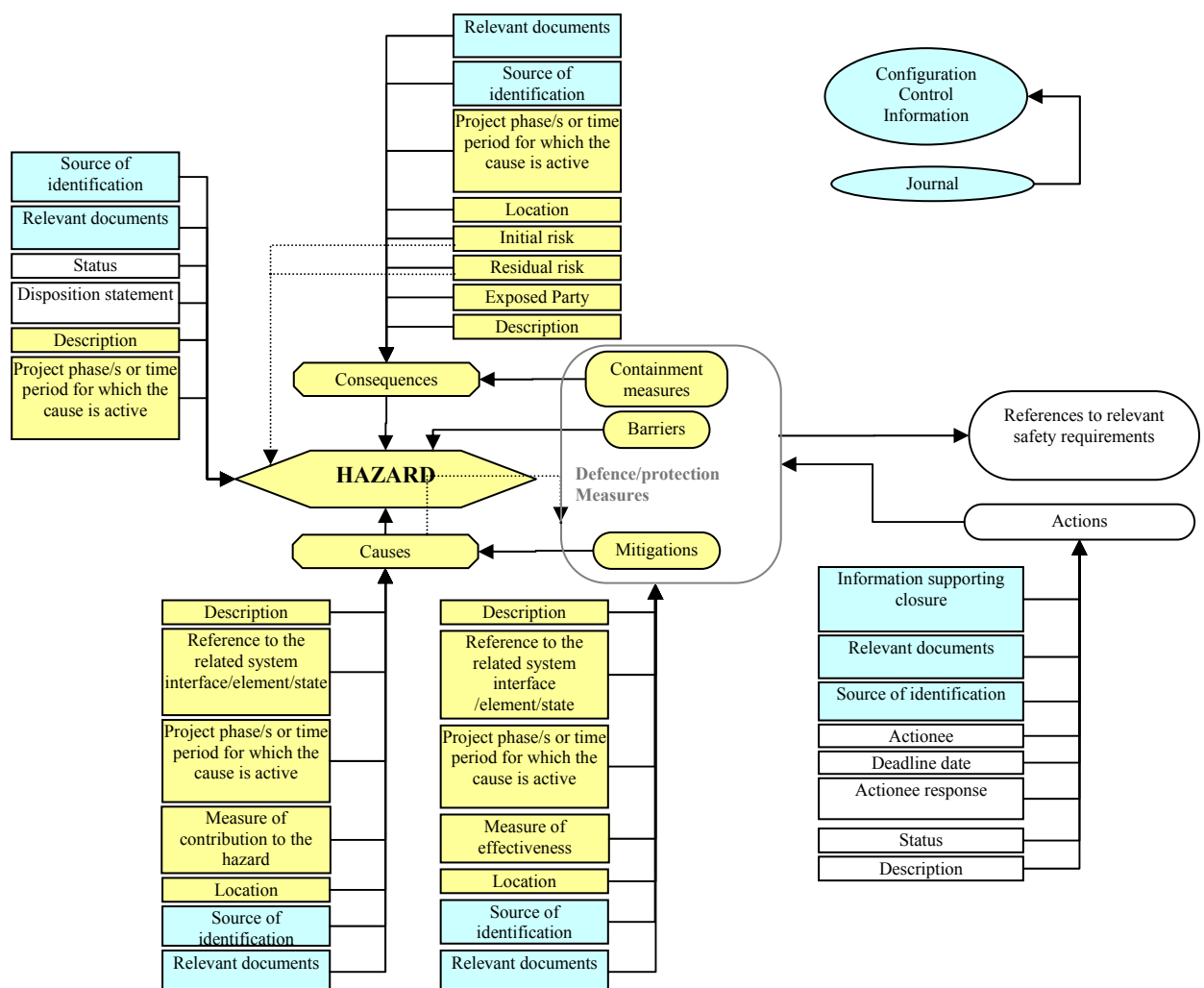


Figure 6-3: Hazard attributes (coloured yellow), information items (blue for audit trial related items and white for management of actions related items) and their relationships

Based on this structure it is possible to define different “views” on our knowledge base about the “hazard universe” under scrutiny.

The “views” will depend on the need of the viewer or interested party. As already discussed, an analyst will be interested in slightly different information than for example a project manager or a person responsible for implementation of identified action or a requirement.

This structure is used for further analysis and development of a process for information gathering, conceptualisation and representation in support of systems safety analysis and management.

6.3 The Safety Case

The purpose of the safety case is to present the arguments that the system, which is the subject of the safety case, is acceptably safe to operate in a precise operational environment (Kelly and Weaver, 2004).

Each safety case consists of four elements:

1. Objectives or Requirements: The safety case must identify and present the requirements that need to be fulfilled to ensure satisfactory safety performance of the system;
2. Evidence: The Safety case needs to present the evidence that requirements are fulfilled;
3. Arguments: The safety case need to present two types of arguments. Firstly it needs to argue that the set of identified requirements is sufficient to secure, assuming that all requirements are implemented, that the system is acceptably safe. Secondly, arguments that the evidence provided that the requirements are fulfilled, is sufficient proof of requirements implementation;
4. Context: The safety case must be defined within the operational context of the system. Therefore the safety case must identify and outline the operational environment of the system being analysed. This needs to include the technical “operational envelope” of the system operating within the given environment under given operating conditions.

As result of the research the author proposes that, from a reasoning point of view a process supporting derivation of the safety case is of a form of the Singerian inquiry. It is possible to present the Singerian inquiry system with the following model:

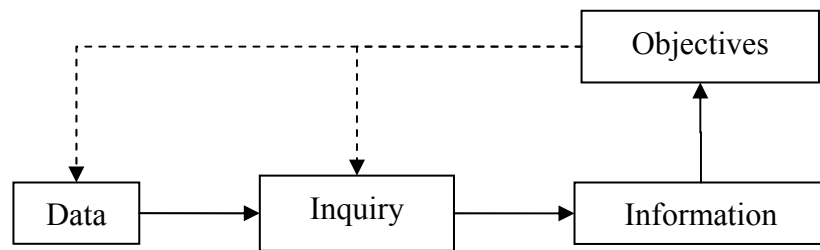


Figure 6-4: Singerian inquiry system model

In the Singerian inquiry model, choice of objectives determines the choice of data to be used and the structure of the holistic inquiry model.

Following the same approach as to the development of the system, system representation and identification of boundaries between subsystems/constituents of the system, to support the above listed constraints, and according to the Singerian inquiry model, the safety case should be structured around main safety goals, objectives, of the system and then decomposed into lower level goals and requirements.

It is possible to treat a safety case derivation process as a system on its own right. If the generalised description of a system, as mentioned earlier, is used, a special case of that system would be a “safety case derivation process system”.

The “safety case derivation process system” is a conceptual, hierarchical system, made up of information packets linked together into a fact net model, with a function to infer and present the reasoning why the undertaking which is an object of the safety case is sufficiently safe.

In the generalised system description information, energy and action as three general categories of inputs and outputs of the system were defined. Also, a special class of inputs and outputs of the system related to environment was identified. In case of the “safety case derivation process system” elements of a generalised system definition can be characterised as follows:

1. The system corresponds to the “safety case derivation process system”;
2. The environment corresponds to the analysed system, context within which the safety case is being developed, legal constraints and societal perceptions;
3. The system constituents correspond to a number of different “objects” as follows:
 - a. The safety goal, or on a lower level of a hierarchy, the safety objective or safety requirement. The safety goal is influenced by external inputs such as legal requirements or constraints and societal perceptions and expectations to mention some;

- b. The data, which in case of safety case process relates to raw information being analysed, or to evidence. The data is taking as an input information from outside the “safety case derivation process system”, from across the system boundary;
 - c. Inquirer, which in safety case process terminology relates data to the information to produce arguments;
 - d. The arguments, which in safety case terminology relates to arguments supporting the claim that the safety goal has been achieved;
4. With regards to the interfaces of the system, three categories were identified earlier, “information”, “action” and “energy”. In a case of a “safety case derivation process system”, since it is a conceptual system, interfaces of “energy” and “action” category do not exist as such. All of the interfaces are in fact “information” interfaces, relating arguments and evidence to safety goals, safety objectives or requirements. In case of external interfaces these are providing data to support the enquiry process and information to mould the safety objectives;
5. The topology of the system corresponds to the structure of internal and external interfaces of the “safety case derivation process system”.

Extending the same principle the “safety case derivation process system” within its environment, can now be presented by Figure 6-5, as follows:

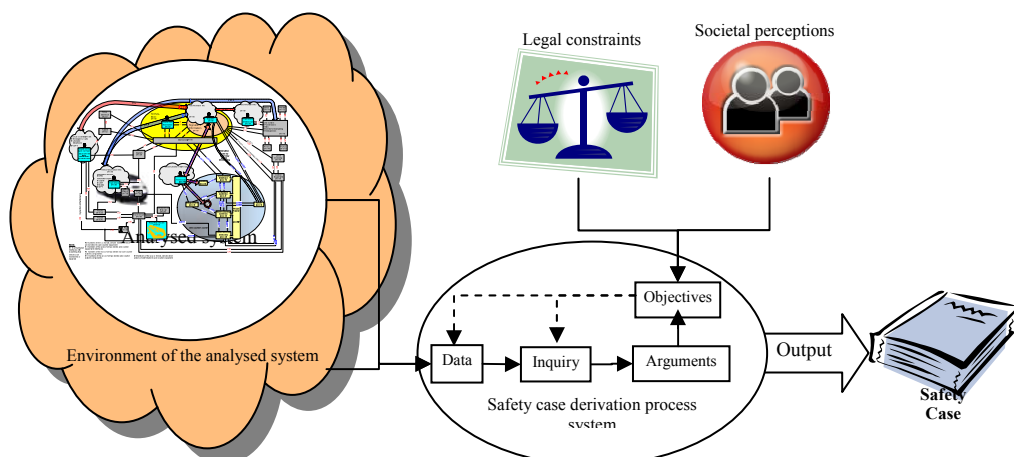


Figure 6-5: “Safety case derivation process system” within its environment

Since the “safety case derivation process system” is in fact the Singerian inquiry model, the choice of objectives will influence the choice of the inquirer and the sought after data. It is consistent with current practice that, when analysing software related systems or subsystems, different methods will be used, than if the subsystem is hardware based. Therefore different inquirers of the “safety case derivation process

system” make up a hierarchy of inquirers related by higher level inquirers into a final argument supporting the objective. Figure 6-6 depicts the extended knowledge net that “safety case derivation process” is.

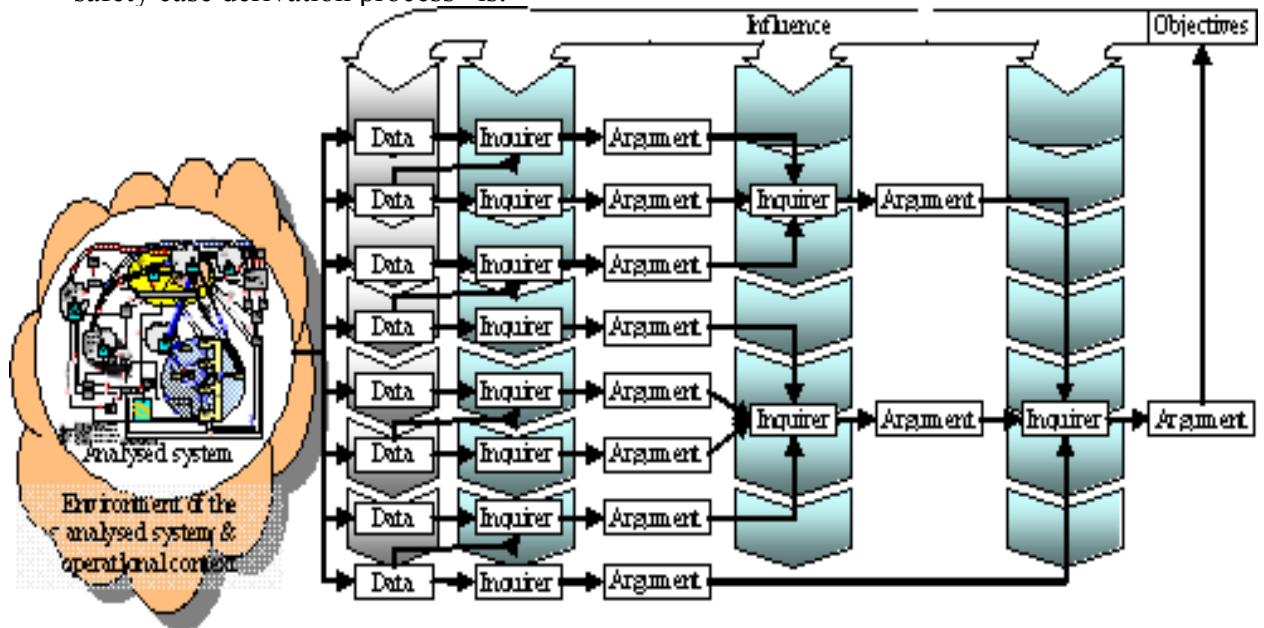


Figure 6-6: Generic safety case derivation process system

The conventional safety case development method is focused on a static system definition, where for any change to the system configuration, a new bespoke safety case needs to be developed (Kelly, 2001).

However modern systems and recent large scale projects introduce additional complexity of a changing system configuration and the environment within which the system is operating (the system here is understood to be the wider system including the operators and users). If a conventional approach to the development of the safety case is to be followed, it would mean that for each system configuration, or stage of the project, a new bespoke safety case would have to be produced.

A more appropriate approach would be to develop a safety case structured in modular elements, which should enable an easy way to adopt or change the safety case to represent each new reality.

In the interest of efficiency, economy and the effectiveness of the safety assurance process, the safety case for each system configuration or project stage, should be structured in such a way as to enable:

Constraint 1. Reuse of material and the structure of safety case supporting the previous system configuration or the preceding project stages to the maximum extent which is appropriate and feasible;

Constraint 2. For each following issue of the safety case, the underlying safety

argument should build upon the safety arguments, safety processes and safety management activities as developed during the previous stages of the project or in support of earlier system configurations.

In support of this approach the author identified two potential methods to structure the safety case “net model”. Firstly, one could partition the system into parts following some predefined methodology, and structure the safety case around these parts (Kelly, 2001). This way, the final safety case would in fact, consist of a number of lower level safety cases, one for each part of the system, brought together by an overarching argument that the overall system is safe.

This approach appears as the most logical way to define a structure of the safety case “net model”, primarily because it is a direct extension of the conventional systems engineering approach.

However, this approach brings about a number of complex requirements that have to be fulfilled:

1. To support the two constraints above clear boundaries between the parts of the system to be supported by the safety case need to be identified. There cannot be any overlaps between the parts, as for each part a safety case will need to be built²;
2. Since the partition of the system requires clear split between different parts of the system, it is necessary to identify all parts of the safety case that depend on the input from other parts of the safety case (mentioned above) and decision has to be made in which part these will be treated;
3. Decomposition of the analysed system also needs to consider the real system boundaries which may be changing throughout the life of the project or the product;
4. Since the first assumption about the analysed system is that it is a changing system and as we need to analyse the impact of the change to overall system safety performance, it is likely that this approach would necessitate complete review of the safety case each time and detailed identification of changed parts in need of a new safety case.

² In practise this are often not referred to as safety cases, but as parts of the overall system safety case. However each one of these possesses all the attributes of a standalone safety case.

An alternative approach is to identify a common “theme” across all different phases of an emerging project or all different manifestations of an evolving system. From early stages of the project onwards, for any system it is possible to identify the Core Hazards emerging from that system. For example, on railways one of Core Hazards would be “Inappropriate separation of trains”. Furthermore, it is very rare that the system to be implemented is so novel that it is not possible to research the history or to use previous experience to identify a comprehensive list of potential Core Hazards. However this is an iterative process and completeness of analysis should be assured through a systematic analysis and review process as is explained in following sections of this thesis.

An overall Safety Goal is that for all Core Hazards emerging safety risks are managed to an acceptable level. Therefore, for each Core Hazard, a safety case like argument should be made to prove that the risk brought about by a particular Core Hazard is managed to an acceptable level.

This approach has several significant advantages. The “safety case derivation process system” is about proving that the emerging safety performance of the analysed system is satisfactory, and its output, the safety case is about presenting the results of the analysis in a logical manner. Therefore, it is logical that the “safety case derivation process system” is structured around the Safety Goals and analysis of the related Core Hazards, as it is successful management of the Core Hazards that define the level of safety risk.

This approach should also make it possible to identify the parts of the subsystem relevant to a Core Hazard and analyse them in the context of that particular Core Hazard. For each new manifestation of the system, a review of the system elements that contribute to the Core Hazard should be undertaken to identify those that are changing. The analysis then can focus on the analysis of changes of the system elements³ and the impact of these changes on the overall safety performance. In order to satisfy the two constraints described above, the structure of the “safety case derivation process system” net model and consequently the safety case arguments needs to allow easy identification of the parts that are changing from one system manifestation to the next one and impact of these changes on the overall system safety performance.

³ Term system element is here used in a wider possible sense, to include the system constituents, interfaces and environment.

Goal Structuring Notation (GSN) as a presentation of the net model lends itself very well to this task. Each of the main elements of the safety case, Objective, Argument and Evidence, as noted above, is represented by a symbol. Notably, Context as a part of the safety case is not presented uniquely by a GSN symbol (Figure 6-7). The Constraint as a symbol of the GSN is reserved for any type of constraint on the system and therefore includes the Context of the system operation. Other symbols of the GSN will be discussed later in this thesis.

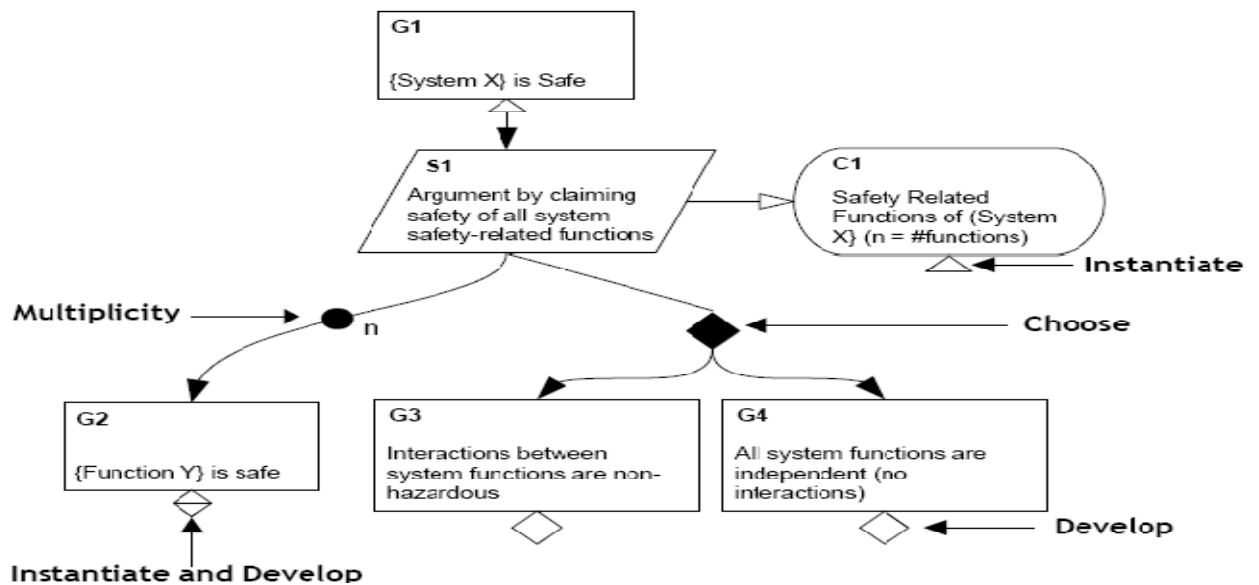


Figure 6-7: Example of reusable GSN pattern

In terms of a structure and specific areas of interest to be covered by any safety case, a structure recommended in EN50129 and the Yellow book (RSSB, 2007) standard is widely recognised as representing a good practice in the production of safety cases and is used well beyond the Standard’s nominal scope of electronic systems for railway signalling.

The following are generic sections which correspond to the four elements of the safety case listed above:

1. Introduction: High level safety objectives or requirements should be presented in this section;
2. System Definition: A safety case can only “exist” within a context of the system for which the safety case is being written. This part relates to a bullet point “4. Context” above;
3. Quality and Safety Management Reports: In support of the safe system operation it is important to develop and implement an adequate Quality and Safety

Management Systems. This part of the safety case should present the Quality and Safety Management System adhered to during the life cycle phases of the system to be supported by the safety case. This part of the safety case tallies with a bullet point “2. Evidence” above ;

4. Technical Safety Reports: This section of the safety case contains all safety reports related to the system. This section corresponds to main safety case parts, Objectives or Requirements, Evidence and Arguments. The context of this section should not be a simple repetition of the previous two sections but should go into much more detail;
5. Related Safety Documents: This section should contain references to all other related safety documents used in support of the development of the safety case.

Later in this thesis it will be show how the structure of the safety case recommended by EN50129 can be fused with the approach suggested above.

6.4 Holistic Change Safety Analysis, Risk Assessment and Management Process

6.4.1 Engineering Safety and Assurance Process – Big Picture

Change Safety Analysis and Risk Assessment Process is the part of the overall Engineering Safety and Assurance Process (ESAP). The author developed ESAP as a generic System Integration process. For clarity, firstly the ESAP will be depicted and, following from there, detail of the Change Safety Analysis and Risk Assessment Process will be provided.

It is difficult if not impossible, to know what the outcome of complex change to a complex system is. The system emergent properties can lead to novel, atypical, dangerous failures. Furthermore, the exhaustive testing of complex systems is most often an impossible task. Hence, the only pragmatic technique to ascertain entirety of the “hazard universe” must be centred around a systematic analysis process.

A process flow diagram on Figure 6-8 describes the information flow, for each major system configuration (related to different project implementation stages), and, at a high level, the inputs, key activities and outputs of the overall systems integration process.

At the centre of the process is the System Definition which describes how the elements of the system relate to one another to provide an integrated system, metamorphosing from one system configuration to the next.

Initial requirements capture brings together all of the known sources of safety, functional and performance system requirements that were documented at the beginning of the project, including the original concept specifications.

Based on these requirements, the system definition is developed to capture the baseline system configuration, before any changes brought about by the project, and subsequently for each of the project stages.

The high level system definition is in the form of a physical architecture diagram depicting the high level architecture of existing systems. Underlining the system architecture, based on the understanding of existing interfaces, the System Context and Interface Diagrams (SCID) were developed.

As the performance of the interfaces defines the performance of the system for each of emerging properties/categories a system is delivering against: safety, RAM and performance, the detailed information about the interfaces, including the stage of the project (system configuration) the interface is active for, is captured in the Objects (assets, procedures and people) and Interfaces Database (OIDB).

The system definition is utilised to analyse the implications of the change on the system and identify detailed requirements against the deliverables, including, Systems Safety, RAM, Human Factors, Operational Readiness, EMI/EMC and Performance.

The first step towards obtaining acceptance of the new system is demonstration that what has been designed meets the requirements as specified during the course of development.

This is done through verification and validation. The aim of the verification is to show that a specification at one stage in the delivery life cycle is consistent and compliant with the specification of the previous stage, taking account of any agreed changes or variations.

Maintaining formal control over the traceability between the requirements repository (DOORS software package) and the project remit and standards enables the project to prevent requirements creep, substantiate its argument for acceptance of the deliverables and identify any changes to the system performance.

Subsequent stages of verification should be between requirements sets and system definitions produced at each stage of the programme/project life cycle (architectural design, system design, sub-system design and detailed design). Validation is undertaken to demonstrate that what has been built against the design meets the stated

requirements.

During the course of systems development all parties involved in delivery of the changes under the project will be compiling evidence that the processes have been followed, safety and performance issues are well understood, and the system to be delivered meets all requirements and specifications.

Consent to move to each new system configuration is sought by an “application to consent to operate” or “consent to trial operations”, supported by an Engineering Safety and Assurance Case (ESAC), which sets out the justification for the assurance of the system, as it is at that stage.

The ESAC presents the arguments for the assurance of the overall system in a given major configuration as affected and delivered by the project works.

The ESAC outlines the system assurance argument by bringing together four distinct areas of assurance:

1. System Safety;
2. Operational Readiness;
3. System Reliability, Maintainability and Availability (RAM);
4. Performance.

Structure of the system safety case is discussed later.

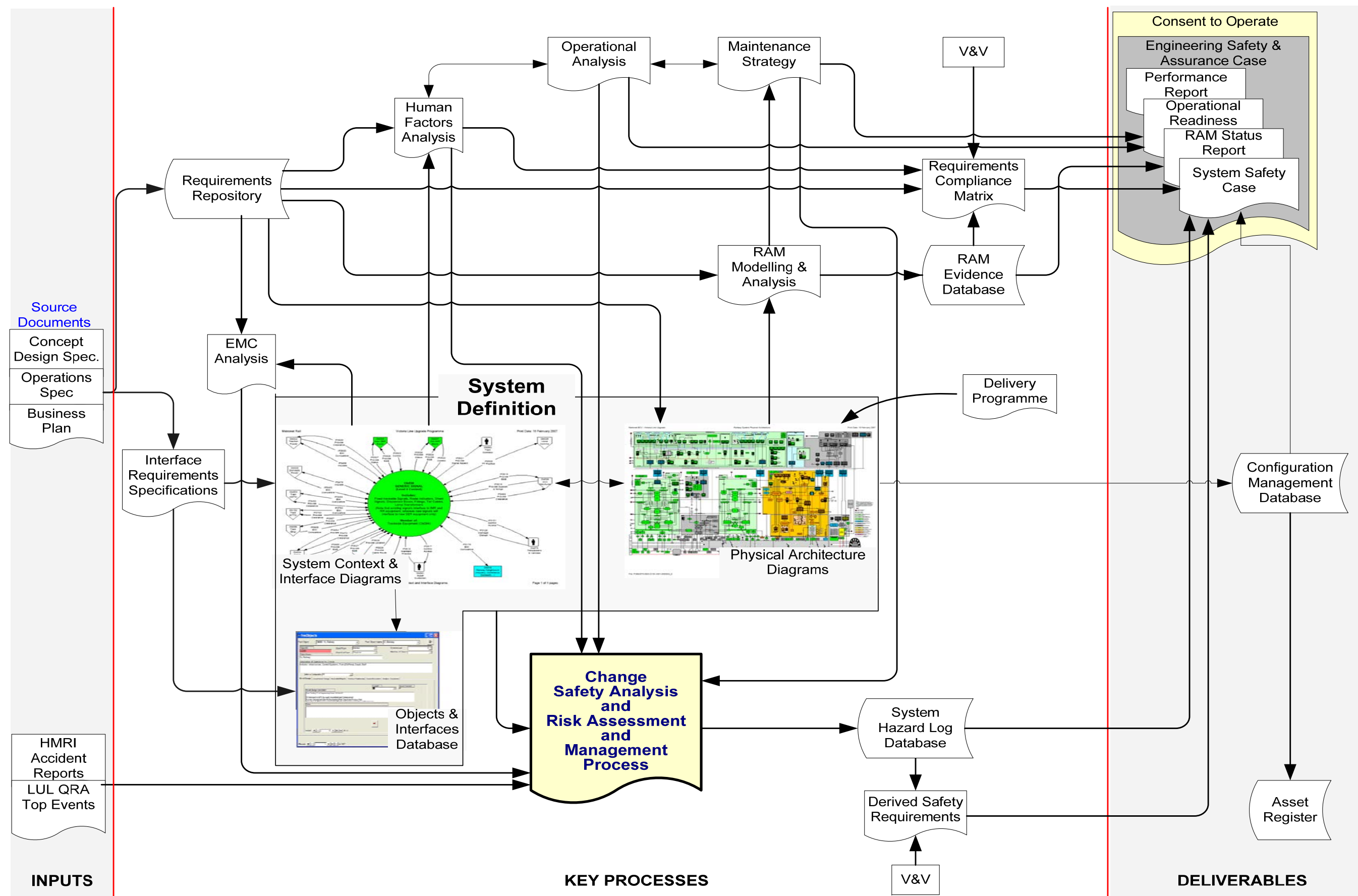


Figure 6-8: Engineering Safety and Assurance Process

6.4.2 The Change Safety Analysis and Risk Assessment and Management Process

The complexity of modern undertakings necessitates an integrated approach to system safety hazard management, quantification of system safety requirements and system safety assurance. The process described in this thesis aims to integrate these three aspects of System Safety Management. To demonstrably discharge the duty of care, it must be ensured that all changes are subject to safety analysis, that a robust process has been followed for the management of system safety hazards and that all hazards have been satisfactorily resolved. However these changes vary enormously in significance and, unless the safety analysis processes are scaleable, they will either impose an unacceptable overhead on the less significant changes or fail to cope properly with the more significant ones. A scaleable change analysis process, the Change Safety Analysis and Management process (provides the framework for achievement of these goals) as defined earlier, is extended to include quantified risk assessment modelling and systems safety requirements derivation, quantification and management. The Change Safety Analysis and Risk Assessment and Management Process encapsulates the following:

1. System conceptualisation and core hazards grouping;
2. Scoping of the impact of the change on safety performance of the system;
3. Safety risk analysis and assessment:
 - a. Hazard Identification;
 - b. Cause Analysis;
 - c. Consequence Analysis;
 - d. Loss Analysis;
 - e. Safety requirements derivation;
4. Qualitative and Quantitative derivation of safety targets and valuation of safety requirements;
 - a. Options and Impact analysis;
 - b. Apportionment and risk profiling;
 - c. Impact assessment and optimisation;
5. Management of safety requirements;
6. Configuration control;
7. Necessary outputs/reports;
8. Input into construction of safety arguments network;
9. System Safety Hazard Log management.

Figure 6-9, below, depicts the CSA, Risk Assessment and Management Process, including the hazard management process and the identified dependencies and the deliverables. The process is heterogeneous and adaptive to any system and encapsulates following activities, dependences/inputs and deliverables:

1. The main input to the process is the System Definition. The system definition is used to scope and baseline the system and initiate the analysis process;

2. As the undertaking is progressing, the initial requirements are subject to changes and these changes must be assessed for impact on the system definition and the system definition should be updated accordingly. Typically on a project these should be done through the Engineering Change Request (ECR);

3. Usually one of the main reasons for change of the initial requirements set is the feedback from initial testing of the system recorded in the Defect Recording and Corrective Action System (DRACAS);

4. Using the system definition information the system is conceptualised, resulting in the set of process models of the system, to enable further quantified and qualitative analysis;

- 5 and 19. The system model is then used to support the Initial Change Safety Analysis and development of the QRA. Output of this activity is the Initial Change Safety Analysis record. This record is configuration controlled and represents one of the building blocks of the completeness of the analysis assurance;

- 6, 18 and 23. Those changes that are categorised as category one or two are subjected to Change Safety Analysis (CSA), all novel changes to the system are subjected to safety analysis Therefore, like for like replacement of existing equipment is not subjected to safety analysis. Output of the CSA process is in the form of briefings, in preparation and support of the analysis and the reports detailing findings of the CSA;

- 7, 21, 22, 23, 24 and 25. Outputs of the CSA provide input into the System Hazard Log. The scale and complexity of the project necessitates a central system hazard data store, referred to as the System Hazard Log (SHL), in support of the derivation of the safety case. The System Hazard Log is the central repository of all the data related to the CSA process and the tool for management of the actions related to implementation of identified mitigation measures. All hazards are entered into the SHL and hazard closure requires review and endorsement at the Hazard Forum. Actions to implement requirements and

mitigations/containment measures are managed and tracked through the SHL as well. From the SHL, System Hazard reports are produced in support of the System Safety Case submission, depicting the status of the SCA activities and the SHL. System Hazard Log Reports are produced quarterly and provide detailed overview of the content and status of the SHL. A significant part of the safety arguments and evidence enabling closure of the SHL records and completion of the Systems Safety Case will come from the safety documentation produced by the supply chain. Finally, results of the System Hazard Log Implementation audits are fed to the SHL and into the System Hazard Log Implementation audits;

-
- | | |
|-------|---|
| 8, 16 | System conceptualisation and the outputs of the SCA are used to support |
| and | quantified or qualitative risk assessment, for each identified Core Hazard. |
| 17. | It should be noted here that a choice of the risk assessment methodology (quantitative versus qualitative) depends on the nature of the risk being analysed and the needs of the safety analysis; |
-
- | | |
|----|--|
| 9. | Both, the risk assessment models (quantitative or qualitative) and the System Hazard Log are “synchronised” in terms of information and coverage of the hazards; |
|----|--|
-
- | | |
|-----|--|
| 10. | Safety requirements should be derived from the defence/protection measures stored in the SHL and some of these requirements will be quantified using the Quantified Risk Assessment model. A Safety Requirements Forum should be formed, to assemble sufficient expertise necessary to elicit safety requirements; |
|-----|--|
-
- | | |
|-----|---|
| 11 | Risk assessment is done at two levels, firstly overall system safety |
| and | performance targets are established, and then the requirements quantified. It is |
| 12. | also necessary to check that results from testing and monitoring systems comply with the quantified safety targets; |
-
- | | |
|--------|--|
| 13, 14 | A team of experts in required disciplines, independent from the project, |
| and | oversee critical CSA activities, endorse the output (reports) of the process and |
| 15. | approve the change of status of SHL actions and consequently the Core Hazards. In support of the Hazard Forum’s decision making, for any change of the SHL action status a proof of implementation is sought in form of an actionee response, V&V report, test log, etc. |
-

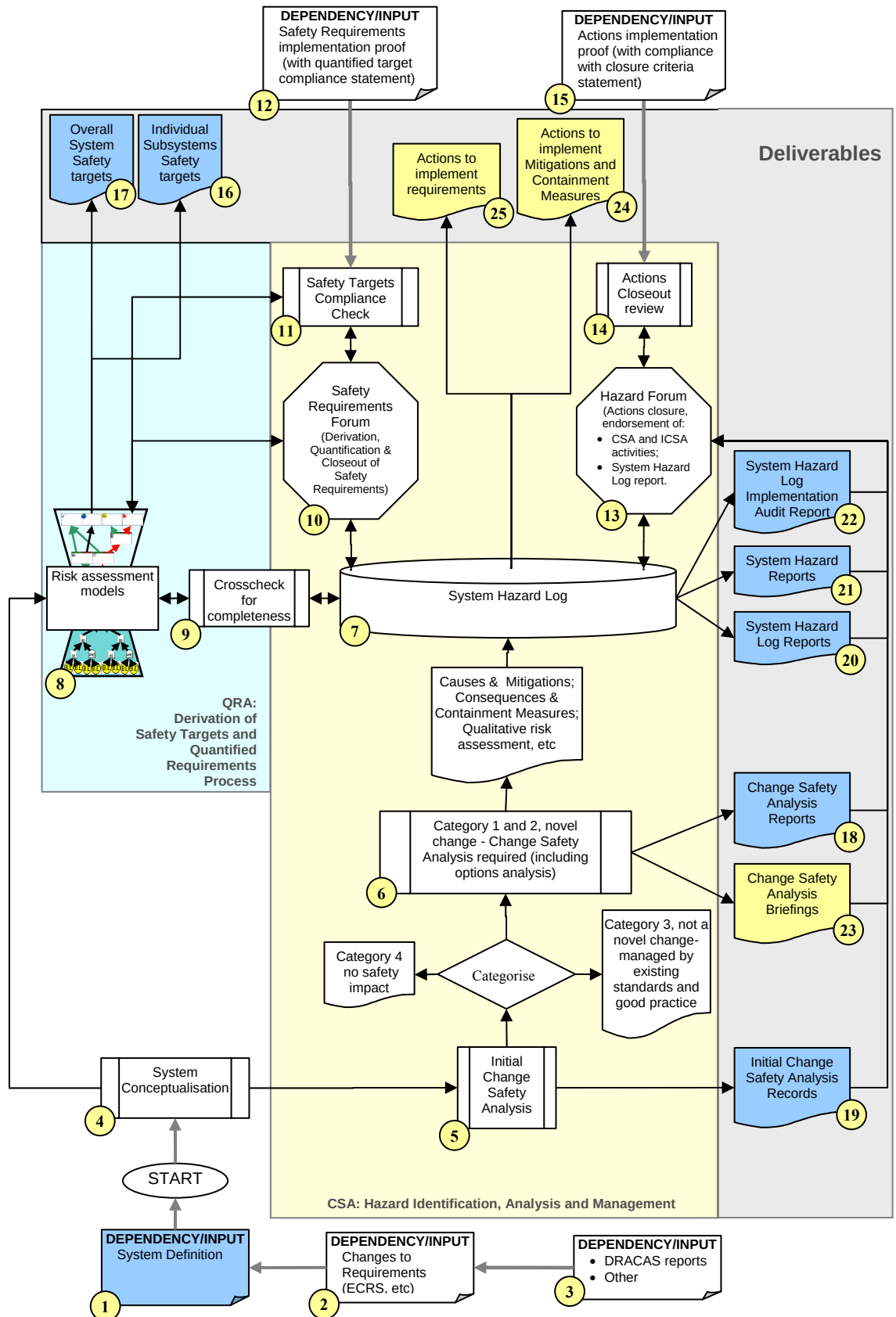


Figure 6-9: CSA and Risk Assessment Process

Detailed description of each step of the process is provided in the following sections.

6.4.3 Conceptualisation and Core Hazards Grouping

To enable the systematic analysis of any system it is necessary to understand the whole of the system, to conceptualise the system. Earlier, several different methods of conceptual modelling were discussed and also some of the applications for conceptual modelling were presented.

For a complex system it is usually necessary to produce a hierarchy of conceptual models, very detailed representations of the system to capture all of the system constituents and their behaviour (these models will be referred to as System Concept Interface Diagrams (SCID)) and higher level system representations capturing the subsystems and their interactions. Still some of the system architecture models contain hundreds of interfaces and objects and are very difficult to analyse and configuration control. For example a System Definition for the Victoria Line Upgrade Programme (VLUP) ⁴, consists of three major elements:

1. Physical Architecture Diagrams, which represent the physical assets and their relationship for all stages of the project as it transforms through different system configurations;
2. System Context and Interface diagrams which model all system constituents including human interactions and the environment;
3. Objects and interface database which contains detailed description of all objects and interfaces within SCID and descriptions of changes to these for different system configurations.

In support of the conceptualisation process a new type of modelling was suggested. If one defines the “core” hazards for the analysed system, then it is possible to extract from the detailed system description (SCID), only those parts of the system that are contributing to the core hazard and produce a conceptual model describing relationships between all of the system constituents (including environmental inputs). Through analysis of historical data and a high level system analysis it is possible to identify the “core” hazards, and use them for grouping of hazards and process models.

The concept of the process model methodology was developed by Short of Atkins Global (Short, 2007), in support of the development of safety cases for complex railway systems.

⁴ Victoria Line Upgrade Programme was used to test the processes described in this section of the thesis. This work is depicted later, in chapter “Application” of the thesis

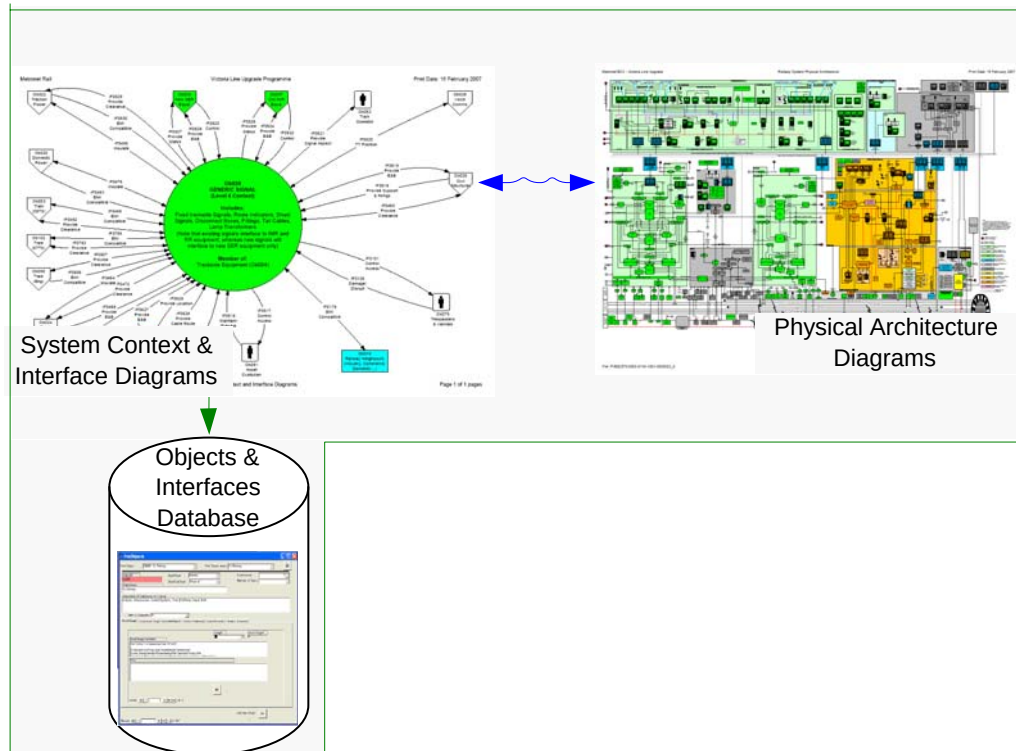


Figure 6-10: An example of System Definition

In line with earlier definition of the system constituents' interfaces being categorised into Information, Energy and Action type interfaces, the system constituent symbol consists of a rectangle depicting the system constituent and three separate partitions of the rectangle, one for each interface type, as shown below on the Figure 6-11.

The agreed convention is that the interface type is defined on the source side of the interface, as it is the source system constituent that defines the type of the interface. Environment is treated as a special type of the constituent.

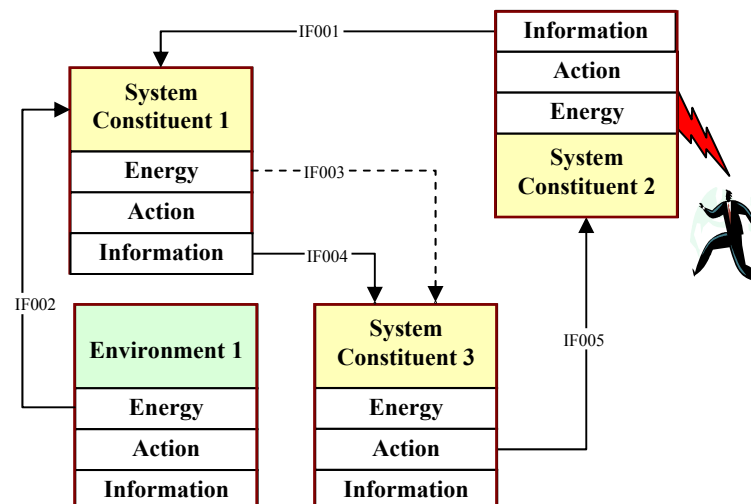


Figure 6-11: An example of the basic Process Model

Further formalisation of this methodology is introduced as part of the research, as follows:

Interfaces can be grouped into intentional and unintentional.

Intentional interfaces are planned, designed interfaces, for example communication link between two subsystems. This is why an intentional action or information type interface can only potentially be an indirect cause of the hazard or the consequence, and hence can only lead to the unintended or uncontrolled release of energy, in case of its failure to perform desirably.

Unintentional interfaces are not planned and appear either by mistake in design, project implementation or as a result of a system failure. An interface that is not intentional is potentially a direct or indirect cause of a hazard or a direct or indirect cause of a consequence. It is only an unintentional interface of energy type that can be a direct cause of a safety consequence (in a sense of uncontrolled or unintended release of energy). An action or information type unintended interface can only be an indirect cause of the hazard or the consequence, and can only lead to the unintended or uncontrolled release of energy.

Therefore, on the process models it is possible to distinguish between:

1. Intended interfaces (annotated by black full line, for example comms link between the signalling system and on board computer);
2. Unintended interfaces that are indirect cause of the hazard or the consequence (annotated by black dashed line, for example Electromagnetic Interference) and
3. Unintended interface that is a direct cause of the consequence (annotated by a red lightning bolt).

All of the Process Model interfaces are described at the level of approximation adopted for development of process models. This description needs to include all changes to the interfaces to be implemented by the undertaking. Furthermore, it is suggested that the process model interfaces should be further “tagged” using a four dimensional classification system:

1. Primary classification: what is the function provided by the interface, or what is the purpose of the interface, reason for its existence;
2. Secondary classification: “being” of the interface, or a method of its execution;
3. Tertiary classification: temporal and operational nature of the interface, or when is the interface active, including all of the operational modes of the system;
4. Quaternary classification: physical environment of the interface, or what is the surrounding of the interface.

A set of generic classifications for a railway system have been developed and is detailed later in the thesis.

Since at the level of approximation of Process Models, some or all of the interfaces are conceptual or composite (for example communication between the train driver and a signaller on the process model would typically be presented with a single line, interface, whilst in reality there are several different methods for this interface to occur, train radio, signal post telephone) further cross-referenced to SCID interfaces, for detail and traceability is required.

It is of utmost importance to develop these models at the appropriate level to ensure that all relevant interfaces are included in the analysis, but also to make sure that the level of analysis is not too detailed in order to avoid the loss of focus on the system analysis as opposed to detailed constituents analysis.

To ensure completeness of the Process Models it is proposed to develop a SCID as a detailed system description model, as already discussed above and then identify clear boundaries between main system constituents, taking into account the engineering and operational aspects of the system as well as commercial/contractual boundaries related to the supply chain and the system constituents being supplied by different provider

SCID and Process models are used in support of the information gathering process and are inseparable as a system presentation tool.

Later in this thesis the experience of use of the process models technique will be discussed and further formalisation will be proposed.

6.4.4 Initial Change Safety Analysis

Initial change safety analysis is done at two levels. Firstly when system definition is established, each of the boundary interfaces identified within the process models should be subjected to Initial Change Safety Analysis (ICSA) as already discussed earlier. This is essentially a structured review process, interfaces are systematically reviewed by a group of experts against predefined criteria as explained earlier.

As part of the ICSA, in support of the future Change Safety Analysis, following information should be collected:

1. Description of the change to interface;
2. What is the rationale behind the way in which the changes are applied;
3. What is the intended purpose of the new function;
4. What is the environment in which the new equipment will be installed;
5. What does the new equipment interface to;

6. What non-equipment changes, if any are being made at the same time (for instance, changes to the maintenance regime or operational rules);
7. Which aspects of the equipment and its application are novel and which have been proven in service;
8. Safety benefits of the change, if any;
9. ICSA category.

As a project is progressing it is inevitable that the intended system definition will change, different subsystem constituents may not be fully compatible or new requirements may be identified, resulting in a different system configuration being brought into existence than the one that was planned. The SCID and process models must be updated to reflect these changes and each of these changes must be subjected to ICSA.

6.4.5 Change Safety Analysis

The Change Safety Analysis aims to integrate an integrated approach to system safety hazard management, quantification of system safety requirements and system safety assurance.

The Change Safety Analysis and Risk Assessment Process encapsulate the following:

1. Change Safety Analysis:
 - a. Identification of Hazard, Causes, Consequences and Defence/Protection measures;
 - b. Analysis of Causes;
 - c. Analysis of Consequences including Loss Analysis;
 - d. Analysis of Defence/Protection measures;
2. Risk Assessment;
3. Derivation of Safety Targets and Quantified Safety Requirements;
4. Change Safety Management.

Identification of Hazards, Causes, Consequences and Defence/Protection measures

As argued earlier in the thesis, the hazard identification is the key phase of the safety analysis of any system. The knowledge gathered during this phase is a base for further analysis. The most important facet of the safety analysis is completeness. It is necessary to assure that the whole system has been analysed and that all aspects of the systems behaviour have been scrutinised. To demonstrate completeness of the analysis, it is necessary to approach CSA systematically.

As previously discussed, a result of standard hazard identification is usually a linear collection of records that fit into different parts of the hazard space: hazards, causes, mitigations, consequences or just project/product issues not directly related to safety performance of the analysed system. Usually, regardless of the method used to support it, the quality of the outcome of the HAZID/HAZOP study, depends only on the skills and experience of the person in charge of the study and his/her ability to control and guide the participating experts. Most of the time, material gathered during these studies requires a significant amount of post processing and structuring.

With the aim to provide the structure to the HAZID/HAZOP studies and enable comprehensive understanding, the following approach is suggested:

1. Since the process models are already produced for each core hazard, identification of hazards themselves is already being done as part of conceptualisation. The first step of the CSA is to subject those interfaces that are classified as ICSA 1 or two to Change Safety Analysis (CSA) to identify related Consequences, Causes and Defence/Protection measures and, for those Defence/Protection measures that are not implemented yet, identify the Actions to implement them.

During the CSA it is useful to follow the guide words [Table 4-7] as it provides additional structure to the analysis. Also, it is necessary to consider all operational modes the system may operate within (normal operation, emergency, degraded mode, failed mode, et.) and different phases of a lifecycle (design, operation, maintenance commissioning/implementation, decommissioning, disposal).

Obviously if, as part of the CSA, a new core hazard is identified, the process needs to be reassessed, new process models produced for these core hazards and the process should recommence;

2. It is essential to keep the traceability from interfaces defined within the SCID to the interfaces of the Process Models and to the identified Hazards, Consequences, Causes and Defence/Protection measures. This will enable rigorous change control and assessment of:
 - a. Impact of any changes to the original scope on safety analysis done thus far; and
 - b. Impact of changes on the safety performance of the system.

Causes

Attributes of Causes are already defined earlier in the thesis, therefore here we will focus on methodologies for analysis and assessment, identification of the relationships and possible combinations between the causes.

It is proposed to make distinction between three areas of analysis:

1. Characterising the Causes.

The aim of this activity is to define the Cause in terms of its description, origin, location and period/time when it is active.

This is done as part of CSA. Description of the cause must be clear and sufficiently detailed to allow further analysis. Since the CSA is carried out by systematic analysis of process models' interfaces, identification of the origin and spatial and temporal characteristics of the cause is in fact mapping of these characteristics from the originating interfaces to related causes;

2. Assessing the measure of contribution of Causes to a Hazard and subsequently to consequences arising from the hazard.

Detailed discussion about this analysis is provided later in section on Risk Assessment;

3. Correlating/Associating the Cause with other Causes, Hazards and Defence/Protection measures.

It is often the case, that failure of a same interface (failure of a function provided by the interface) may lead to more than one hazard or it is necessary for some other interface to fail in order for this, now combined failure to lead to a hazard. Also some of the causes will actually lead to failures of Defence/Protection measures.

It is necessary to identify all of these relationships in order to comprehensively understand the effect of the interface failures or in other words, Causes, on the overall system.

Analysis of causes could be supported in line with several different methods for example:

1. FMEA/FMECA (see earlier discussion) is usually performed at the detailed design level, whereby an analysis of the design is undertaken to identify potential failure modes. This approach can be utilised for analysis at the system level;

2. Reliability Block Diagrams and Network Models (see earlier discussion), again are methodologies usually utilised for detailed analysis at design level to identify common mode failure modes and enhance system redundancy.

Consequences and Loss

Understanding of the potential consequences of a hazard is a prerequisite to appreciation of the risk and therefore management of it.

Attributes of consequences have already been discussed, as well as different approaches to estimation or calculation of probability or frequency of consequence occurrence and loss analysis.

Therefore, here the author will only discuss several aspects of the analysis of consequences and losses as follows:

1. It is necessary to define the location of consequences and their temporal nature as part of the initial identification. For example if a consequence happens only during out of normal service hours, the loss associated with that consequence could be much less than if it happens during peak hours when exposure to the consequence is much higher;
2. As part of the initial analysis relationships between the consequences should be identified. It is possible that a consequence is actually a secondary effect of some other consequence, or that a consequence always materialise simultaneously with some other consequence.

It is also important to identify the nature of subsequent loss in terms of safety, commercial and environmental loss and the exposed party (service users, service operators, neighbours).

Defence/Protection Measures

Mitigations, Barriers and Containment Measures and their attributes are already defined earlier so here we will focus on only on aspects of identification and analysis not already discussed earlier.

Assessing the measure of effectiveness of Defence/Protection Measures is a vital enabler of conclusive ALARP argument. Assessment of effectiveness of Defence/Protection Measures depends on comprehensive understanding of:

1. “Being” of these, in terms of their origin (are these measures a physical thing, an alarm for example, a planned human intervention such as scheduled maintenance or circumstantial event);

2. The temporal and spatial nature of the Defence/Protection Measures, or when and where these measures are active and effective;
3. The potential relationship between different Defence/Protection Measures, for example it is possible that a Defence/Protection Measures is effectively working “against” one hazard but may actually contribute to another (increase number of maintenance checks for example may reduce a number of equipment failures but may increase exposure of staff to occupational hazards);
4. Reasons for, or causes of, failures of the Defence/Protection Measures as these may be related to causes of a Hazard as well.

Risk Assessment

Quantitative versus Qualitative

Both of these approaches have been discussed in detail earlier and it is not the intention to detail the techniques and different methodologies for risk assessment here.

Both approaches are equally legitimate and informative and each suffers from some common and specific limitations.

The main shortcomings of quantified risk assessment (QRA) are cost (often the cost of this activity cannot be easily justified, particularly for simple undertakings) and lack of reliable data (particularly if the undertaking is about a novel and/or complex change). On the other hand, qualitative risk assessment often results in unsubstantiable argument based around informal estimates of consequence occurrence and associated loss. In addition to that, some problems are very difficult if not impossible to model, for example system failures related to human action and software performance, without experiential data being available.

As already discussed earlier, it is often possible to develop a substantiated quantified risk assessment model of an existing system, and in this circumstances, most of the time it is possible to obtain valid data to support modelling of this existing system. It is valuable, as it is rarely the case that the whole system is introduced as a completely new novel system. Most often, the undertakings are about the existing systems (for example railway system) being upgraded or improved through either a number of small changes in time or a substantial large scale upgrade programme. In these cases it is possible to develop the QRA model representing the safety performance of the system before any changes to the system are made. This approach permits an initial model to be populated with valid data and gauged against the validated historical data. This model can then be used as a base for development of a model representing the

effect of the changes to the system and impact of these changes to the safety performance of the system. This approach minimises the amount of new data to be identified/derived and makes it possible to validate the model predictions against a reliable reference point.

However, regardless of how much validation and verification of data is done, in practice use of the absolute value predictions of common QRA models (the most often technique used within the railway industry is the fault tree) in safety reasoning is very arduous to assure and justify.

Most often, in practice, use of the QRA predictions is limited to:

1. Comparison of safety performance of a future system against the safety performance of an existing system. This is always done in relative terms, the outcomes of the two models, are compared and the difference between two outputs is taken as the result of the analysis. This is then used in support of an argument that the safety performance of a future system is in relative terms better or at least the same as the safety performance of an existing system. In case that the analysis shows that the safety performance of a future system is worse than that of an existing system, further analysis and changes to the future system are to be done until the results are favourable. For more detail on this please see the next section of the thesis;
2. QRA models are often used to set/derive initial targets for a developing system. Later on, once the constituents of the system have been developed and tested, real data can be fed back into a model to confirm that the overall safety target has been achieved.

Where a qualitative approach is applied, it is suggested that instead of an absolute estimate of the risk a comparative approach is taken, as described earlier in section “Complex Railway Project Safety Management – Manchester South Capacity Improvement Project”. It is along the same line of reasoning, adopted for the QRA modelling; if a reference point is defined and used for measurement of risk the claim for assurance of the assessment should be built around the comparison with the a known risk profile. Using this methodology greatly enhances the quality of expert estimates; qualitative assessment is almost always based on knowledge of domain experts and inference.

In its nature the Inquiry System suggested here is a Lockean Inquiry System, the problem domain is an empirical one, building arguments into a fact net, based on a set of empirical judgments elicited from domain experts.

Apportionment, Optimisation, Options and Impact analysis, Amalgamation of Quantitative and Qualitative Analysis and argumentation for selection of options for implementation

Systematic study, of each hazard, regarding the causal and consequential effects of failures shall be carried out. In order to identify all the applicable defence/protection options, the best available expertise shall be employed. Results of apportionment and importance analysis are used as guidance for concentration of effort and prioritisation of options analysis.

To enable rigorous option suitability assessment, for each identified option following information must be provided:

1. Cost of implementation;
2. Timescale for implementation;
3. Need for additional training;
4. Impact of implemented option on a selected consequence;
5. Impact of the selected option on the overall safety performance forecast by the model.

This information will provide a basis for the decision making process and support the ALARP argument.

As explained, both approaches to risk assessment, Quantitative and Qualitative, have some limitations, mainly caused by difficulty in obtaining reliable data to feed into the reasoning model. To overcome this problem it is proposed to use both approaches, to complement each other, in support of the safety risk assessment and justification.

In general, construction of the safety argument should be carried out around two lines of reasoning (Health and Safety Executive, 2009):

1. Demonstrating that the safety performance of a new or changed system is at least as good as the safety performance of a similar or previous system (before any changes being done to it).

Ethically and legally, we expect the new or enhanced system to deliver at least as good safety performance as the previous one. With the rapid advance of technology and science it would be impossible to justify increasing the societal exposure to risk, the expectation is to improve safety performance with time.

Using the QRA methodology in support of this line of reasoning is beneficial and is compatible with the approach detailed above.

2. Demonstrating that the owner and/or the beneficiary of the undertaking has reduced the safety risk emerging from the system to As Low As Reasonably Practicable (ALARP) level.

Ethically and legally, it is expected that the risk of any undertaking is mitigated/controlled to an acceptable level. In the UK in particular the acceptable level of risk is defined as ALARP. This requirement calls for identification of the controls of hazards on an individual basis (for each hazard) including consideration of all possible controls. It is only when there is nothing else, practicable, that can be done to reduce the risk level further, that the safety risk emerging from the system can be considered as ALARP.

To support the argument that the safety risk emerging from the system is ALARP it is necessary to demonstrate the practicability argument by carrying out a cost-benefit analysis to assess and compare the costs of any proposed changes to the system against the reduction in risk levels inclusive of the acceptance/rejection criteria.

It is proposed here that the analysis should be done at two levels:

- a. For specific highly critical hazards (ones that have major contribution to safety risk) the QRA approach is recommended, but only if it is possible to develop QRA models representing the system before changes or a similar already existing system so that data and the model predictions can be validated and verified.

The QRA should then be used in support of the options identification and analysis and the ALARP argumentation.

- b. At the system level, for each hazard, a qualitative/comparative methodology suggested earlier (please see section “Complex Railway Project Safety Management – Manchester South Capacity Improvement Project”) should be applied.

This methodology allows for a systematic and transparent assessment of all hazards and related causes and defence/protection measures. However, in order to enable the process it is necessary to structure the hazard log in such a way as to make it possible to comprehend relationships between

different elements of the “hazard universe” and to ascertain sufficient information to support domain experts in their review and estimation of risk.

Derivation and Management of Safety Requirements

In recent times with advance of systems engineering, management of interfaces between system constituents, suppliers, contracts, internal divisions delivering parts of the system, etc. is executed through management of system requirements. The system requirements should say what the system must do, not how it must be done, and should be set at the level of interfaces across boundaries within the system, where the boundaries are defined as boundaries between major system constituents and system and environment. The boundaries may be dictated by contractual arrangements for delivery of the system constituents, internal divisions into delivery groups on the project, etc. Regardless of the reasons behind the structure of the project delivery organisation, these influences must be taken into account when system boundaries are defined within the system architecture and/or process models as described earlier.

Following from the change safety analysis process, Safety Requirements should be derived from identified defence/protection measures. However, not all of the defence/protection measures are capable of being translated into requirements. Some defence/protection measures are simply statements of fact, and although valid, these are not worthy of being transformed into requirements. For example, the Victoria line of London underground is wholly underground in a deep tunnel. It never rains on Victoria line and this is a good mitigation against corrosion, but it is not a requirement. Furthermore, in line with the approach taken regarding the change safety analysis process, if the change is conventional (like for like replacement or introduction of already proven and used technology, there is no need to define detailed requirements as such, a reference to existing standards and good practice should suffice. On the other hand, introduction of a new signalling system demands systematic identification of all related requirements, including safety requirements, and methodical management to validated and verified implementation.

Some of the safety requirements are not quantifiable as such. For example a safety requirement “all train drivers must be trained to drive the train in all operational conditions” is a binary statement, it is either done or not.

If we define a set $\mathbf{M}_h$ of all defence/protection measures (mitigations “m”, barriers “b” and containment measures “c”) of a hazard h to be $\mathbf{M}_h = \{m, b, c\}$, then set of all safety requirements $\mathbf{R}_h$, associated with the hazard h , is a subset of set $\mathbf{M}$; $\mathbf{M}_h \subseteq \mathbf{R}_h$. Furthermore, a set of quantified safety requirements $\mathbf{Q}_h$, associated with the hazard h , is a subset of set $\mathbf{R}_h$; $\mathbf{M}_h \subseteq \mathbf{R}_h \subseteq \mathbf{Q}_h$.

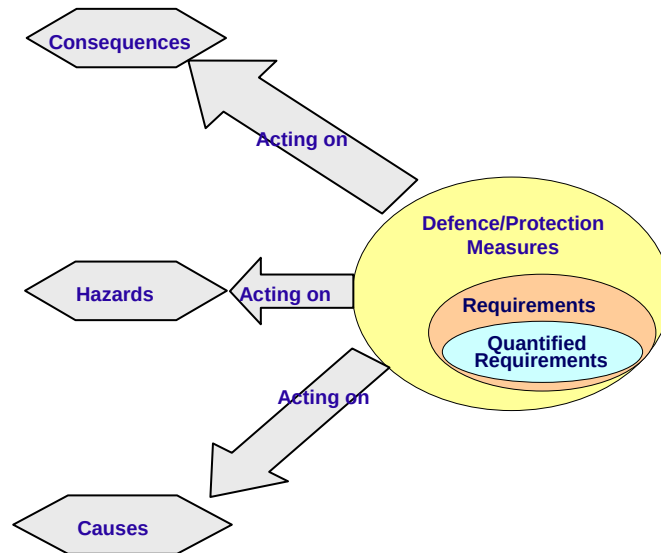


Figure 6-12: Defence/Protection measures, Requirements & Quantified Requirements

Selected defence/protection measure should be stated in the form of safety requirements on performance, function, procedure, environment, competence and other reduction methods. The safety requirements must then be apportioned to those projects and suppliers that are responsible for delivery of the equipment, people and procedures that embody the causal factors identified in the analysis.

The projects and suppliers to which these safety requirements have been apportioned are responsible for supplying the evidence that safety requirements have been met. The System Safety Case is populated with the system safety requirements as apportioned to the projects and suppliers and evidence coming from the projects and suppliers.

The safety requirements are associated with defence/protection measures they have been derived from and should be managed through the hazard log, because implementation of a requirement enables closure of a hazard log entry.

6.4.6 Assertion of Completeness of System Analysis

An essential part of any safety argument is an argument about the completeness of the safety analysis done. In making any logical claim, the most difficult part of the argument is proof of completeness of analysis and understanding of uncertainties involved in decision making. The following are the areas of interest:

1. Completeness of the system understanding:
 - a. understanding of the existing system (system to be changed);
 - b. understanding of the changes to the system to be introduced;
2. Completeness and correctness of change safety analysis:
 - a. completeness of hazard identification and identification of protection measures and safety requirements;
 - b. correctness of risk analysis and assessment and certainty of data used in support of risk assessment;
3. Completeness of the safety arguments/facts net:
 - a. completeness of totality of lines of reasoning explored;
 - b. completeness and certainty of evidence provided in support of arguments.

Completeness of the system understanding

Completeness of the system understanding consists of understanding of the existing system, system before changes and the changes to be introduced to the system and the effect of these changes on the system properties.

The process models have been used on both projects to support this understanding as already explained earlier. Confidence in completeness of the system understanding is achieved through a rigorous process of process models' production, review and configuration control.

Completeness of change safety analysis

There are two slightly different types of completeness and certainty in relation to change safety analysis.

The first type is about the *comprehensiveness* of analysis of the conceptualised system (process models) aimed at identification of hazards, protection measures and requirements.

The second type is about the *correctness* of the risk assessment and analysis of the identified hazards, protection measures and requirements and the correctness of information used in the analysis. It is particularly relevant to QRA and options and impact analysis.

The assertion of comprehensiveness is achieved through adherence to a structured and rigorous process of hazard identification; preliminary analysis (Initial Change Safety Analysis and Change Safety Analysis) is done on the process models of a system as

base-lined and agreed by the project. The analysis must include all of the boundary interfaces identified within the system architecture and mapped to the process models.

Once the system architecture and process models are base-lined, any changes to the system should be controlled. The change control mechanism is usually known as the Engineering Change Request, and is in a form of an official request for change of base-line design. Usually this process is not formalised in a sense of changes being referenced against interfaces, the change is described and the impact of change assessed by competent experts.

However, to comprehensively support ICSA and CSA processes it is necessary to integrate configuration control of the system architectures with the ECR process. It is suggested that each change request is referenced to the interface impacted by the change and submitted to the custodian of the system architecture for impact assessment. Any change to the system should be approved by the custodian of the system architecture and the system architecture/process models updated.

In order to complete the impact assessment, regarding the impact of the change on safety performance of the system and/or effect of changes on safety analysis already done; for each change, affected interfaces should be identified, and then subjected to ICSA and if necessary CSA. Output of this analysis feeds into a hazard providing the base for further analysis and supporting construction of safety arguments.

The assertion of correctness is achieved through adherence to the rigorous and transparent process for development of QRA logic and data collection and review.

However, in this case it is also possible to gain further confidence with regards to the data used for QRA. Use of sensitivity analyses to identify the most critical data items, and focus data search and checking in these areas, use of multiple, independent data sources, comparison of model prediction with real life data (base-lining) are all techniques that should be used in support of building confidence in the modelling results.

6.4.7 Hazard Log, tool for Change Safety Management, Configuration Control and Reporting

The hazard log is a central repository of the knowledge gathered during the analysis and the tool supporting management of activities related to safety analysis and control. All the information gathered through the analysis should be captured in the hazard log. The basic information to be contained in the hazard log is defined in the railway industry guidance, the Yellow book (RSSB, 2007):

1. **Journal** should describe all amendments to the Hazard Log, in order to provide a historical record of its compilation and provide traceability.

2. **Directory**, sometimes known as the Safety Records Log, should give an up-to-date reference to every safety document produced and used by the Project.

It may be convenient to keep the Directory separate from the rest of the Hazard Log, or even to integrate it with a project document management system.

3. **Hazard Data** should record every identified hazard. For each hazard, the information listed later in this section should be recorded as soon as it becomes available. Data collected during Hazard Analysis and Risk Assessment should be transcribed to the Hazard Log when the reports have been endorsed.

If the hazard is not closed or cancelled, then the name of a person or company who is responsible for progressing it towards closure should be captured as well;

4. **Incident Data** should be used to record all incidents that have occurred during the life of the system or equipment. It should identify the sequence of events linking each accident and the hazards that caused it.

5. **Accident Data** should be used to record every identified possible accident. It should identify possible sequences of events linking an identified accident with the hazards that may cause it.

It is easy to see that all of the information listed above has been already identified as part of the overview of the hazard attributes earlier in the thesis. The only outstanding part is reference to Directory and Documents and this is not directly related to identification, analysis and management of individual hazards. The author would recommend that generic documentation related to plans and processes for safety management on the project should not only be included in the hazard log directory, but should be integrated with the project document management system.

Since all of the information gathered during Change Safety Analysis is contained in the hazard log it seems logical to utilise the hazard log to actively support further analysis, not to be only a repository of results of the analysis. If the hazard log is structured in such a way as to present the data in a form of a Meta-model of the “hazard universe”, it then could be used in support of further analysis, for example in support of qualitative risk assessment, review for completeness, or construction of safety arguments.

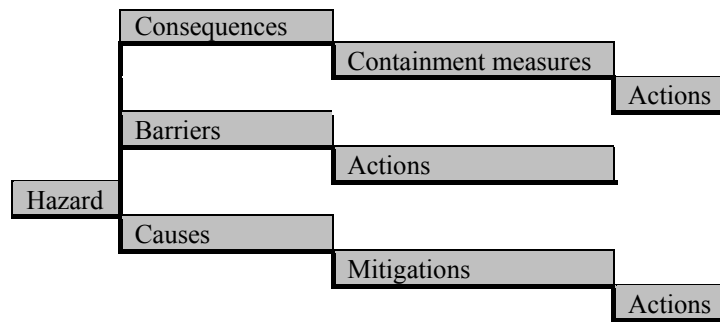


Figure 6-13: Hazard Log Hierarchy

With this in mind a Hazard Log database has been developed. The complexity of the Hazard Log database is due to many – to – many relationships that occur between the different elements of the hazard log, for example, one consequence may apply to many hazards, and one hazard may have many consequences. This cross-fertilisation between the elements lends itself to the capability of cross referencing to other elements by selection. The figure below shows the relationship between the data items (tables) in the Hazard Log:

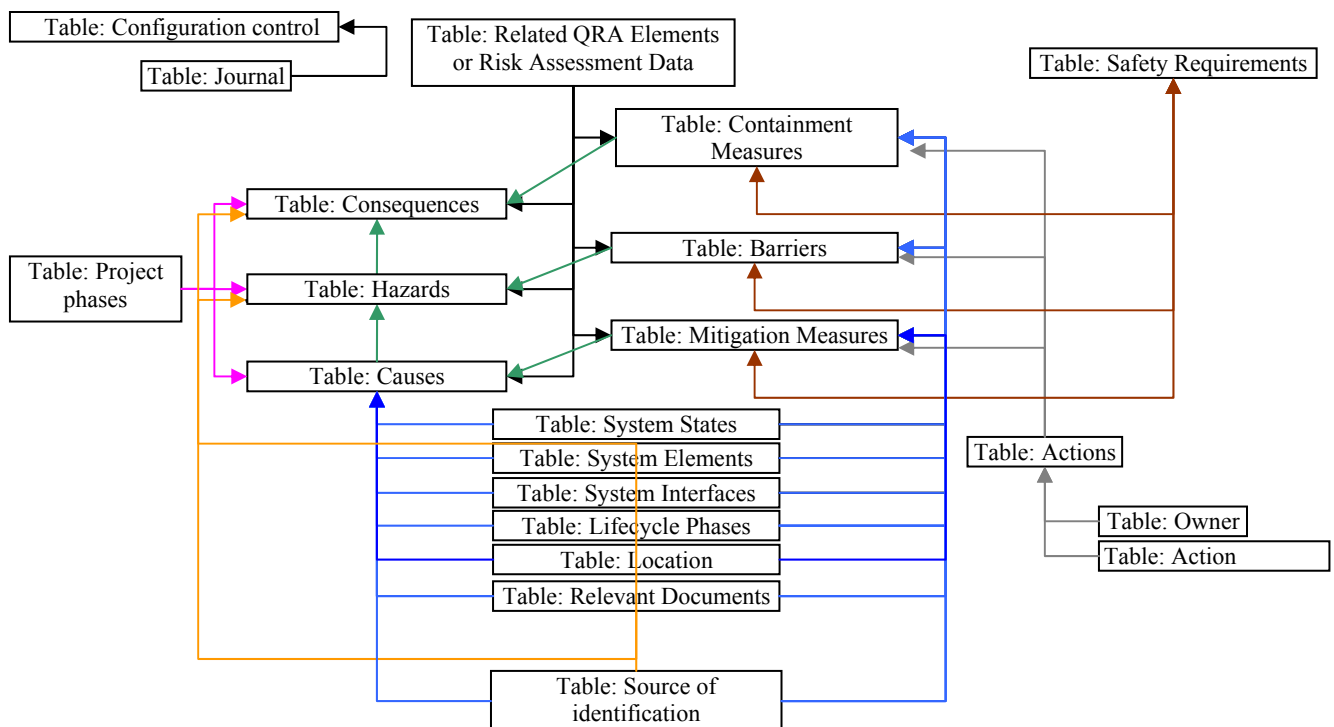


Figure 6-14: Hazard Log relationships

Note: all tables are in one-to-many relationship in direction shown on figure 3 above (for example, one cause can relate to many hazards) except for relationships between:

1. Table: Consequences and Table: Hazards, where each consequence can belong to only one hazard and
2. Table: Configuration control and Table: Journal, where each journal entry can be related to only one configuration control entry.

The following table describes the various elements that make up the Hazard Log and its relationship to other elements:

Element Name	Attributes	Attributes-Relationship to other elements
Hazards	1. Unique Identifier; 2. Hazard Name; 3. Hazard Description; 4. Comments; 5. Disposition Statement.	Many – to – many relationships with: 1. Related Causes; 2. Related Barriers; 3. Related QRA Model Elements (if QRA is used); 4. Pertinent Lifecycle Phases; 5. Pertinent Project Phases; 6. Source of Identification; 7. Relevant Documents; One to one relationship with: 1. Related Consequences; 2. Hazard status (Open; Conditionally Closed; Cancelled; Closed; Transferred); 3. Pertinent Location.
Causes	1. Unique identifier; 2. Cause Name; 3. Cause Description; 4. Measure of a contribution of the cause to the Hazard and related Consequences; 5. Comments.	Many – to – many relationships with: 1. Related Hazards; 2. Related Mitigations; 3. Related QRA Model Elements (if QRA is used) or Risk Assessment Data; 4. Related System States; 5. Related System Elements; 6. Related System Interfaces; 7. Pertinent Lifecycle Phases; 8. Pertinent Project Phases; 9. Source of Identification; 10. Relevant documents; One to one relationship with: 1. Status (Open; Conditionally Closed; Cancelled; Closed; Transferred) 2. Pertinent Location.
Consequences	1. Unique identifier; 2. Consequence Name; 3. Consequence Description; 4. Loss associated with the consequence; 5. Frequency or probability of consequence occurrence 6. Comments; 7. Initial Risk; 8. Residual Risk.	Many – to – many relationships with: 1. Related Containment Measures; 2. Related QRA Model Elements (if QRA is used); 3. Related System States; 4. Related System Elements; 5. Related System Interfaces; 6. Pertinent Lifecycle Phases; 7. Pertinent Project Phases; 8. Source of Identification; 9. Relevant documents; One to one relationship with: 1. Related Hazards; 2. Exposed party; 3. Pertinent Location.
Mitigation Measure	1. Unique identifier; 2. Mitigation Name; 3. Mitigation Description; 4. A measure of reduction of the detrimental effect of	Many – to – many relationships with: 1. Related Causes; 2. Related Safety Requirements; 3. Actions for implementation of mitigation; 4. Related QRA Model Elements (if QRA is used); 5. Related System States;

Element Name	Attributes	Attributes-Relationship to other elements
	- the cause; 5. Comments.	6. Related System Elements; 7. Related System Interfaces; 8. Pertinent Lifecycle Phases; 9. Pertinent Project Phases; 10. Source of Identification; 11. Relevant documents; One to one relationship with: 1. Pertinent Location; 2. Status (Implemented; Not Implemented)
Barrier	1. Unique identifier; 2. Barrier Name; 3. Barrier Description; 4. A measure of reduction of the detrimental effect of hazard 5. Comments.	Many – to – many relationships with: 1. Hazards; 2. Safety Requirements; 3. Actions; 4. Related QRA Model Elements (if QRA is used); 5. Related System States; 6. Related System Elements; 7. Related System Interfaces; 8. Pertinent Lifecycle Phases; 9. Pertinent Project Phases; 10. Source of Identification; 11. Relevant documents; One to one relationship with: 1. Status (Implemented; Not Implemented); 2. Pertinent Location
Containment Measure	1. Unique identifier; 2. Mitigation Name; 3. Mitigation Description; 4. A measure of reduction of the loss; 5. Comments.	Many – to – many relationships with: 1. Consequences; 2. Actions; 3. Related QRA Model Elements (if QRA is used); 4. Related System States; 5. Related System Elements; 6. Related System Interfaces; 7. Pertinent Lifecycle Phases; 8. Pertinent Project Phases; 9. Source of Identification; 10. Relevant documents; One to one relationship with: 1. Status (Implemented; Not Implemented); 2. Pertinent Location.
Actions	1. Unique identifier; 2. Action Name; 3. Action Description; 4. Comments; 5. Action Response 6. Information Supporting Closure; 7. Implementation Deadline; 8. Date Action Allocated; 9. Date Action Completed.	Many – to – many relationships with: 1. Related Mitigation; 2. Related Barrier; 3. Related Containment Measure; 4. Source of Identification; 5. Relevant documents. One to one relationship with: 1. Action Implementation Managers; 2. Status.

Table 6-1: Hazard Log Elements and Relationships

Element Name	Attributes	Attributes-Relationship to other elements
Configuration Control	1. System hazard log version number; 2. Version details; 3. Comments; 4. Issued by	One to Many relationship with: 1. Related journal entries
Journal	1. Journal Entry Reference; 2. Entry created by; 3. Date of journal entry; 4. Comments.	

Table 6-2: Configuration control and Journal data

If the Hazard Log is structure in such a way and contains all of the information discussed above it could be used in support of the following safety analysis and management activities:

1. Structuring and grouping of the identified causes, mitigations, hazards, barriers, consequences and containment measures into Core Hazards' meta models supporting analysis;
2. Management of safety activities through management of actions;
3. Configuration management of safety information and audit trail;
4. Reporting against the status of the hazards analysis, management of safety activities and achieved levels of safety.

6.4.8 Continual Appraisal and Knowledge Update

Through the time of undertaking/project it is necessary to keep the information required to secure safe delivery of the undertaking up to date. This should be implemented through a regular review of changes to the original system design, for example review of ECRs and impact of these changes on the analyses done so far, and the review of data collected by the system performance monitoring processes such as Failure Reporting And Corrective Action System (FRACAS).

During the lifecycle of the project or any undertaking for that matter, in particular in early stages of the lifecycle, in order to initiate analysis it is necessary to make some assumptions, for example about the future performance of the system, or about particular interface behaviour. Furthermore, during the analyses often it is necessary to identify dependences that need to be acted upon prior to operation of the system, and caveats or restrictions setting the limits, defining the boundaries of the operational envelope of the system. These need to be regularly reviewed and updated. A change of assumption may initiate additional analysis or review of analysis already done to

ensure the results are still valid. A change of dependency may cause a change of a schedule, new chain of actions to be implemented and finally, a change in restrictions to be implemented, need to be captured as it is the restrictions that have a significant contribution in defining the safe operational envelope of the system being implemented or changed. For the purpose of management and control of these it is suggested that establishing databases to collate and control Change Requests and Assumptions, Dependences and Caveats (Restrictions) would be beneficial.

6.3 Chapter Conclusions

In this chapter the author presented and discussed the new systems based framework for analysis and management of safety risks that the author developed against the requirements identified earlier in Chapter 5.

In support of the framework, the author analysed the hazard as a system concept and developed existing notions further, identified and defined the attributes, and their hierarchical structure, of a Hazard as a system. The author also analysed the concept of the safety case as the inquiry model identifying a number of constraints and requirements that a safety case must satisfy. Subsequent to analysis of these, the author proposed the general high level approach to structure of the safety case as a fact net, reasoning model.

In previous chapters, the author presented the results of the analysis of the existing system safety and system engineering processes and guidance, and some of the early development results and identified requirements for a new framework. The author outlined the vision of the safety engineering as an integrated part of the system engineering process and the assurance of delivering the needed functioning of the four key emerging properties of any system: safety, RAM, Operability and Performance.

Following from that the author developed and outlined the integrated process for analysis and management of engineering safety. The process consist of 7 steps, most of which are not newly identified as needed but have not been formalised nor used together within an integrated framework.

CHAPTER 7: APPLICATION

7.1 Chapter introduction

The aim of this chapter is to present the results of a real life application of the developed process. The scope includes two major London Underground upgrade projects; the Victoria Line Upgrade Programme and the Subsurface Lines Upgrade Programme, on both of which, the author with his team, is successfully applying the process depicted in this thesis.

As part of the application of the process and methodologies, developed earlier, where need for further enhancements was identified it was completed and is discussed in this section as well.

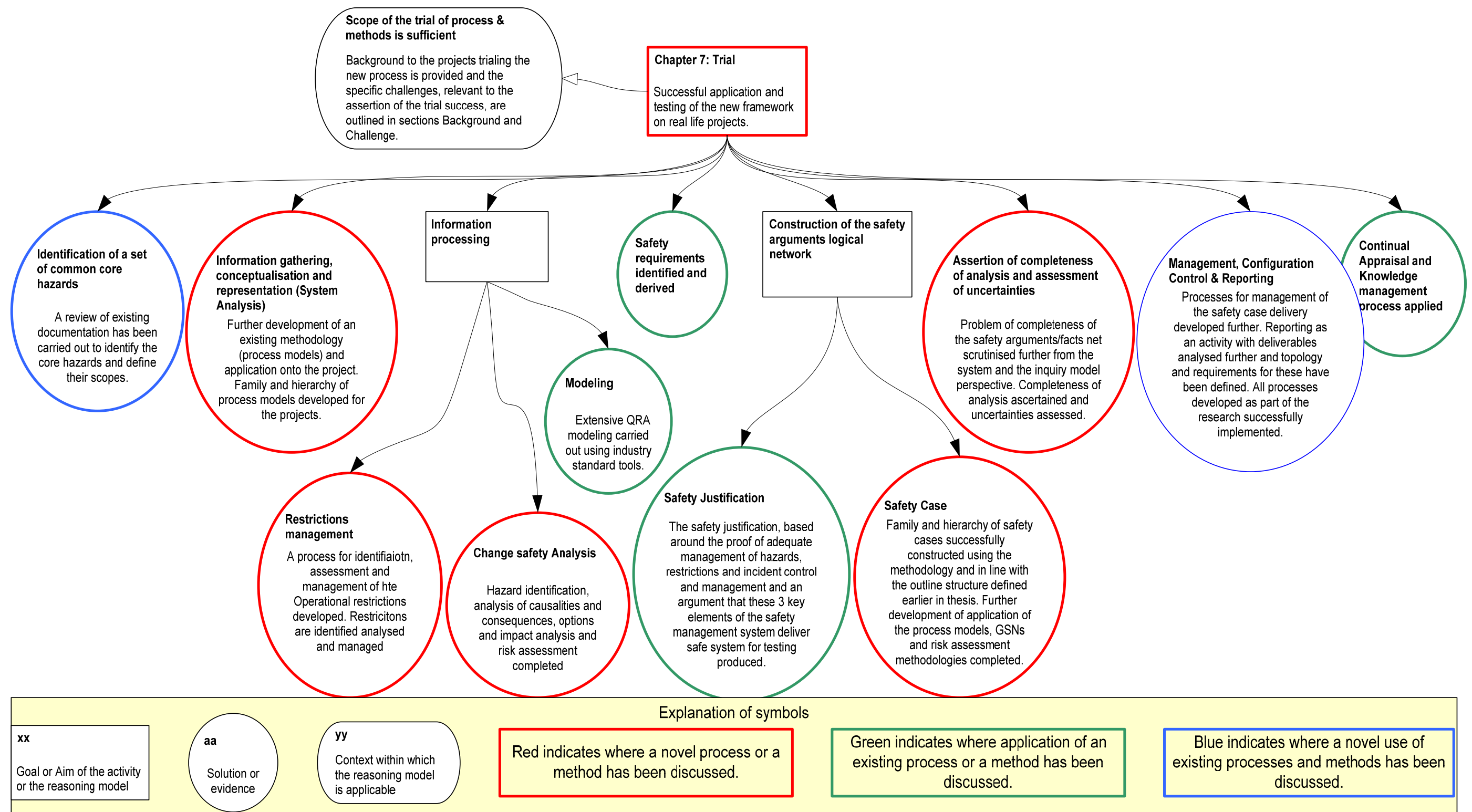


Figure 7-1: Structure of Chapter 7 and argument in support of claim that the newly developed process has been successfully trialled and any shortcomings in the initially developed process developed further

7.2 Background

The Victoria Line Upgrade Programme (VLUP) is a multi-discipline project. The principal works included within the programme are the upgrading of rolling stock, signalling and signalling control. The solution involves:

1. Delivery of a fleet of 47 new trains, to be driven automatically, but with the capability to be driven manually at full speed under Automatic Train Protection (ATP);
2. Delivery of a new signalling system, including:
 - a. Train borne equipment,
 - b. Signal equipment room equipment,
 - c. Control Centre equipment, and
 - d. Trackside equipment.
3. Delivery of a new signalling and communications control systems, located within a new Service Control Centre (SCC);
4. Removal and disposal of existing Victoria Line trains and signalling;
5. Provision of train cab and signalling simulators; and
6. Training in system operation and maintenance and provision of maintenance manuals and full technical documentation.

These works are supported by a number of infrastructure enabling works and support activities. These include:

1. Provision of new Signalling Equipment Rooms (SERs) and cable routes;
2. Provision of new signalling power supplies with battery backup (Uninterruptible Power Supplies);
3. Track upgrade works (through the Metronet Rail Bakerloo, Central and Victoria Line (MRBCV) Track Renewals Programme);
4. Substation enhancements (through the Power Private Finance Initiative (PFI) with EDF);
5. DC power distribution enhancements by the VLUP;
6. Transmission links and train radio enhancement (managed through the Connect PFI);

7. Depot upgrade works;
8. Station upgrade and enhancement - including Customer Information Systems (CIS) (through the MRBCV Stations & Civils Programme);
9. EMC and gauging surveys.

The VLUP is being delivered by a number of projects (around 25) and in a number of major configurations.

To deliver the VLUP, the VLU Project Team within the Victoria Line Programme has been established. The VLU Project Team is responsible for managing all contracts entered into, to deliver the VLUP, for integration of the various subsystems that make up the upgrade and for various other cross-discipline functions.

It is the responsibility of the VLU Project Team to deliver the overall Engineering Safety and Assurance Case (ESAC), comprising of the System Safety Case, Railway Operational Readiness Report, System RAM Status Report and System Performance Status Report.

Bombardier Transportation supply trains, signalling and signalling control.

Bombardier Transportation has a contract with Westinghouse Rail Systems Limited (WRS�) for delivery of the signalling and signalling control, while delivery of trains is the responsibility of Bombardier Mainline and Metros. Bombardier Transportation is responsible for the delivery of these systems and their integration for the VLU.

Subprojects of the VLU Project will carry out the delivery of the Victoria Line Service Control Centre (SCC) building and systems integration, and other enabling works such as track upgrades and SER construction.

Two Private Finance Initiatives (PFI), being managed through separate contractual arrangements by LU, also enable the VLUP:

1. The Power PFI contract with EDF Energy Powerlink Limited - responsible for power supply upgrades by way of substation enhancement;
2. The Connect PFI contract with CityLink Telecommunications Limited - responsible for radio and transmission upgrades.

There is no direct contractual relationship between VLUP and the two PFI suppliers.

Requirements from the LU have been placed on VLUP through the Public Private Partnership (PPP) contract. Any changes to these requirements will need to be negotiated with the client organisation within LU. LU is responsible for providing

safety analyses and assurance evidence from the PFI suppliers to the VLUP to support the VLUP System Safety Case, as required by the VLUP System – wide Work Package Plan.

The VLUP also interfaces with other LU/Metronet Rail/Tube Lines supply chain partners responsible for other London Underground Upgrade programmes:

1. Balfour Beatty - responsible for ongoing track renewals;
2. Stations Alliance - responsible for refurbishment and modernisation of Metronet stations and civil infrastructure.
3. Station upgrades, carried out by Tube Lines.

All of the subsystem suppliers to the VLUP are responsible for safety management within their individual scope of responsibility.

Operation of the line is the responsibility of LU (apart from engineering hours when it is responsibility of VLUP).

Maintenance of the line is the responsibility of LU Maintenance Organisation.

However, initially WRSL will maintain signalling part of the system with planned hand over to LU Maintenance Organisation at later stage.

The Subsurface Lines Upgrade Programme (SUP) consists of many projects that together deliver the capability improvement requirements and PPP contractual obligations to achieve improved Subsurface Lines (SSL) railway performance.

The following major programme of works is to be undertaken for the upgrade of the SSL railway:

1. Replacing the ageing rolling stock offering improved capacity and performance;
2. Replacing the obsolete signalling control system with one offering greater operational management capability and improved headways;
3. Providing a new Service Control Centre (SCC) for LU controllers, ergonomically integrating a number of systems and their human factor requirements including signalling control, train communications, Public Address, tunnel telephone and auto telephones;
4. Providing the necessary power upgrades including the upgrade of low voltage AC power required for SUP and station upgrades, and support LU with the DC traction power upgrade;

5. Necessary infrastructure enabling works such as track, station and depot upgrades including the provision of new signal track equipment;
6. Providing rolling stock (cab) and signalling control system simulators;
7. Training in the operation and maintenance of the new or altered assets and systems provided, as well as maintenance manuals and full technical documentation.

Each SUP Upgrade Steps is delivered through a staged process of translating the system requirements and contractual obligations into infrastructure changes. The final stage, and hence the upgrade of the complete SSL railway, is due to be delivered by March 2018.

The principal objective of the staged process of commissioning the SSL railway is such that:

1. Safety risk is kept As Low as Reasonably Practicable (ALARP);
2. That the risks of the SSL upgrade programme are understood and managed to acceptable levels as the new systems are rolled out;
3. Revenue service is maintained at existing levels, with service improvements as the new systems are rolled out;
4. The operational, technical and functional maturity of the railway is progressively implemented;
5. System rollouts are achieved within the constraints imposed by the access requirements;
6. Roll-out costs are contained within acceptable levels.

The SUP will also interface with three network-wide PFI schemes modernising the SSL infrastructure:

1. Communications - Connect PFI contracted with the consortium known as CityLink. It is responsible for supporting the radio system and providing reliable, high-capacity data links which can be flexibly deployed, a robust fibre-optic transmission network will also be installed. This will provide the SSL Railway with transmission links to support signalling control and communications systems;
2. Power - PFI contracted with EDF Energy Powerlink Limited (EEPL). The new trains and signalling to be delivered by the Metronet programme will require

more power than at present; therefore to accommodate the new trains the high voltage distribution network has to provide more power than is currently available. The PPP contract provides for LU to improve the existing power to meet these needs. With the integrated approach to implementation of both programmes (SSL and Power PFI), this power upgrade will be in place prior to the full-scale introduction of new trains to the SSL Railway;

3. Ticketing - Prestige PFI contracted with the consortium known as Transys. There are few links between the Prestige PFI and the SUP, although there is a need for these to be identified and managed. An example is that many ticket gates in the central area use compressed air from the signalling air main for their motive power; this supply must be maintained despite the decommissioning of pneumatic signalling equipment (e.g. points) on the SSL Railway.

The SSL Programme is required to roll out an extensive upgrade of the 284km sub-surface network over the next 10 years. The upgrade will impact virtually all the assets on the current SSL network and will have a significant impact on the operation and maintenance of the railway during the intermediate and final state of the SSL Upgrade Programme. During the upgrade of the SSL railway, a number of interim railway system configurations is defined, as the new assets are delivered into service across the SSL railway network. In addition to the work needed to manage procurement of the new rolling stock and signalling, additional enabling works are required to allow the new trains to operate on the line. The resulting work has been divided into four principal project portfolios as follows:

1. Train Systems portfolio – All work required for preparation, passenger service, availability, and maintenance of the first S8 trains. This includes S8 trains, necessary depot upgrades, DC traction upgrades including low loss conductor rail;
2. Track portfolio – All work required along the route to enable the S8 trains to interoperate with existing rolling stock at line speed, includes train arrestors, gauging, maximum safe speed;
3. Immunisation portfolio – All work required in some areas of the SSL network to overcome safety concerns over the compatibility of the new trains with the existing train detection equipment. This includes signalling immunisation track circuit replacement, low voltage signalling power, cable route management and communications;

4. Station Enabling portfolio – All work required at stations along the route of the S8 trains to interoperate with existing rolling stock in passenger service. This includes correct side door enable (CSDE), selective door operation (SDO), OPO TT CCTV and platform extensions and modifications.

7.3 Challenge

Organisationally, both major upgrade programmes, SSL and VLU, are split into a number of layers; at programme layer, final integration into a railway system is undertaken whilst constituents are delivered by projects and supply chain, the immediate integration into subsystems is realised by project portfolios which are groupings of related projects.

For example, on the Victoria Line, the train is being delivered by Bombardier Passenger Group; the signalling control is being delivered by Westinghouse. Initial integration of the signalling onto train is carried out by Bombardier London Underground Projects.

Once the train-signalling subsystem integration is completed, the final integration of the subsystem is completed by the VL Upgrade Programme.

This is illustrated by Figure 7-2 below, where blue colour indicates integration at project portfolio level and red colour indicates the programme level integration.

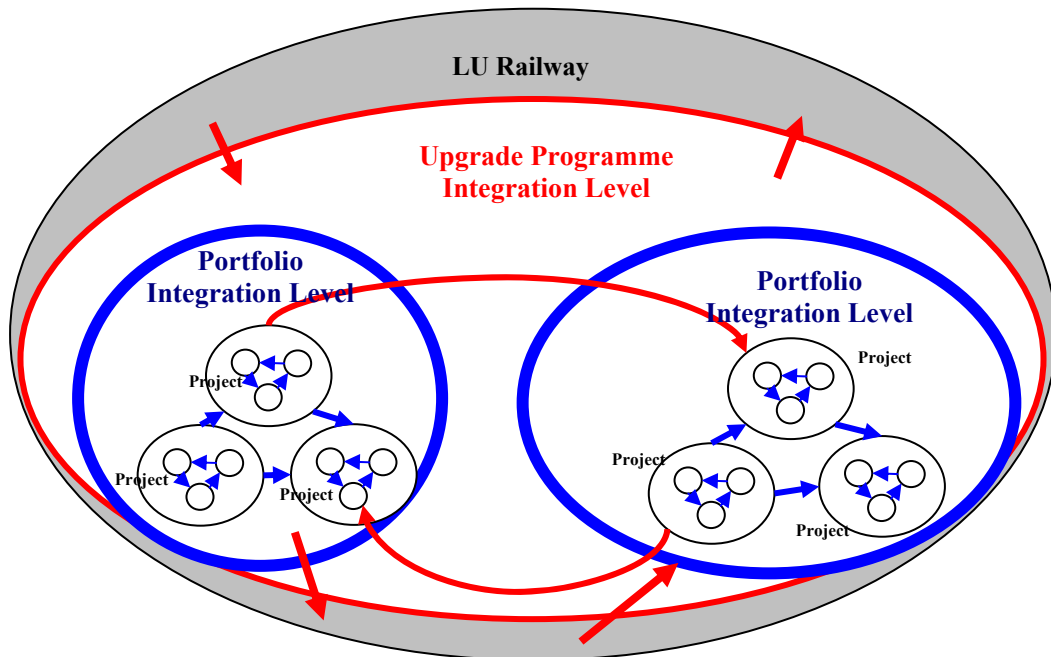


Figure 7-2: Organisational structure of the Upgrade Programmes and two integration layers

Integrating safety arguments from a large number of parts and subsystems integrated into a railway system and all delivered by different projects and long and complex

supply chain, into a series of holistic and coherent system safety cases (one for each of the main system architectures) is a challenge.

The complexity of the Upgrade Programmes necessitates an integrated approach to system safety management.

the author achieved this by ensuring that the various projects, suppliers and project portfolio's, and their specific engineering safety management processes are guided by the common principles and practices (set out in the programme level Engineering safety Management Plan) and interact in such a way that the overall safety requirements and quantitative safety targets are met for each defined railway system configuration state.

As illustrated by Figure 38, there are three areas of focus when implementing the integrated safety analysis management on any complex project, alignment of processes, alignment and coordination of analysis and management activities and harmonization and coordination of deliverables.

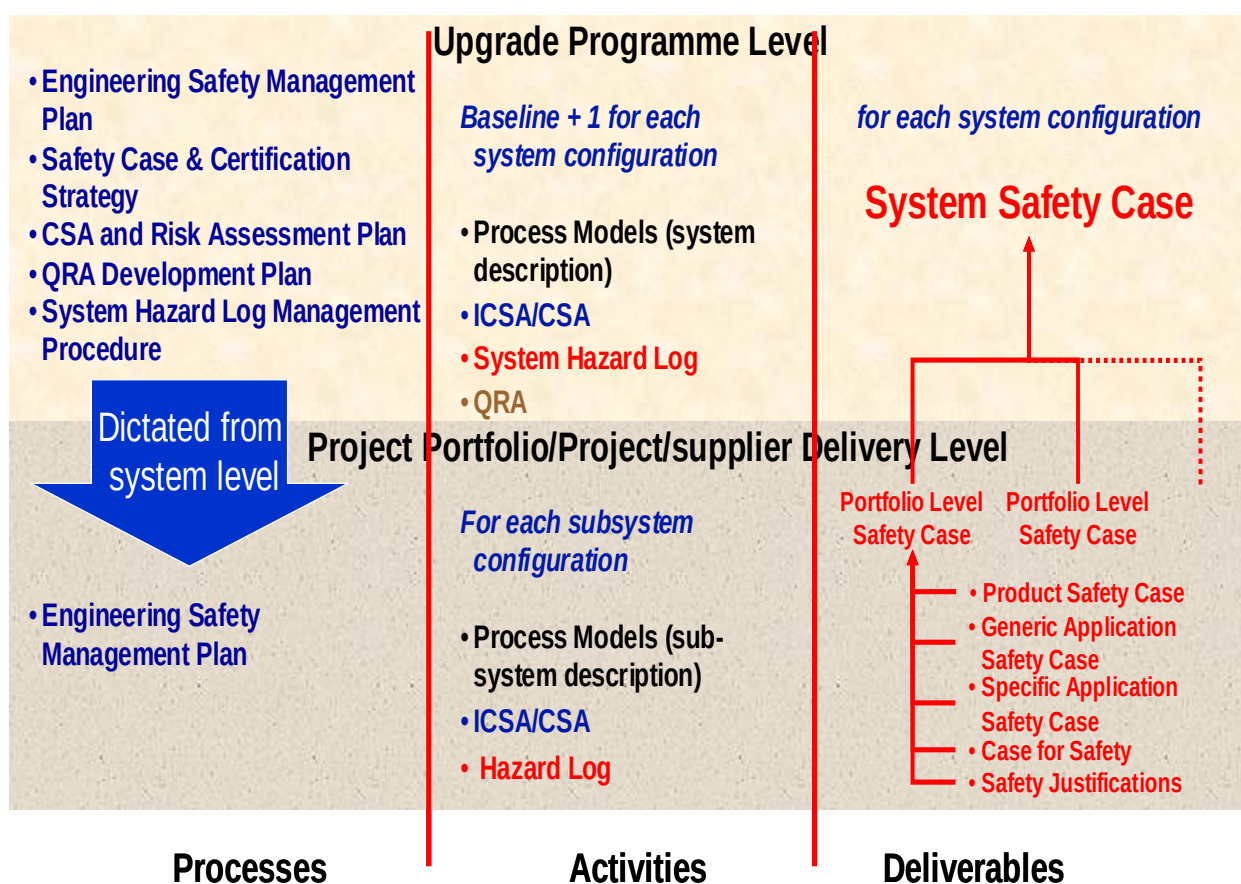


Figure 7-3: Integrated safety management process

When mapped onto the organisational structure of the upgrade programmes, this arrangement can be represented by Figure 7-4 below.

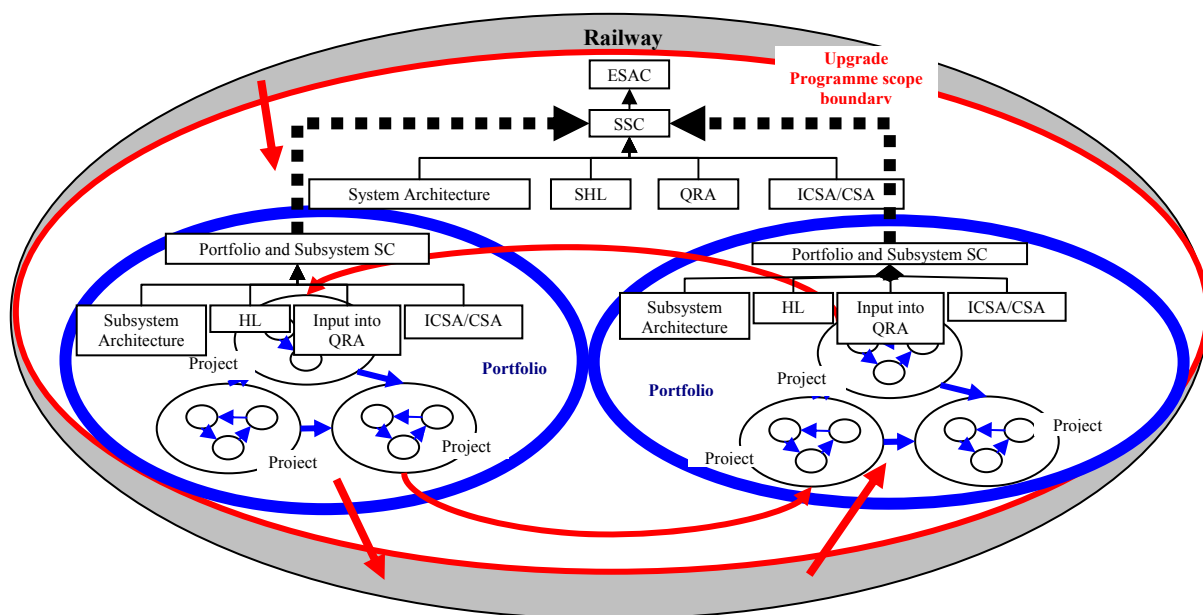


Figure 7-4: Integrated safety management process mapped onto organisational breakdown structure

Following common engineering safety analysis and management fundamentals, based around the safety fundamentals defined at the programme level, are implemented, across the project portfolios and key supplier, to enable an integrated approach to managing and demonstrating system safety for each of the configuration states:

1. **Identification of a set of common core hazards.** To ensure a common approach to hazard identification and analysis it was essential that the same set of core hazards is used as a template structure for hazard log groupings across the programme, at system hazard log level across to the project portfolio-project level.
2. **Use of a hierarchy of Process Models** starting from the system level down to the delivered subsystem/constituent level in order to:
 - a. Define the scope of analysis at system and project/supplier level;
 - b. Facilitate common understanding of the scope of change to be introduced to the railway system;
 - c. Facilitate common understanding of interface boundaries between different projects/suppliers scopes of work;
 - d. Enable the traceability between different elements of the process, namely, QRA, Hazard Log and CSA in support of completeness argument.
3. **Use of the principles of change safety analysis** at programme and project level to identify hazards, mitigations and safety requirements. These have been explained in detail earlier.

4. **Apportionment of Safety targets and quantification of requirements.** To demonstrate that the risks resulting from the changes to the railway are Tolerable, ALARP and no greater than the level of risk in the current Railway System, quantitative risk assessments are carried out, and a set of requirements related to the new hardware system constituents have been quantified.

For purpose of reporting against the risk performance, London Underground developed QRA models of the 20 most critical hazardous events, some time ago. The current London Underground Subsurface Lines and Victoria Line QRA (LU SSL and VL QRA) models are based upon an assessment of the risk of passenger fatalities from the hazardous events. These models have been reviewed aiming to limit the scope of the programmes QRA to only those interfaces and related hazards that are affected by the scope of the programmes' works as defined by reference to the Railway System Architecture.

The subset of LU QRA models has been developed further to establish a baseline set of models representing the Current Safety Performance (CSP) of the SSL and VL prior to any changes introduced by the programmes' works.

Predictions from these models have been used to set Tolerable Hazard Rates (high level safety targets) for both programmes.

The set of CSP models has been further developed to reflect changes to the SSL and VL to be introduced by the programmes, for each stage system configuration and geographical area. As result a series of Interim Safety Performance (ISP) and Final Safety Performance (FSP) models of the SSL and VL have been developed. The models are used to quantify safety requirements for novel parts of the system and to confirm that the Tolerable Hazard Rates (high level safety targets) have been met by each of the programmes for each system configuration during migration.

5. **The use of a consistent hazard management process and hazard log structure** across programme, project portfolio's and key suppliers including implementation of Hazard Forum at programme and Interdisciplinary Hazard Review Group at the project portfolio level.

To demonstrate that risks associated with the hazards introduced to the SSL and VL railways have been reduced to ALARP, a robust hazard management process has been implemented. In addition a clear relationship between the Hazard Logs at the System (Programme), Subsystem (Project or Project Portfolio) and the Constituent (Supplier) level has been established and documented aiming to

adequately manage hazards introduced to the operational railway as a result of the upgrade programmes.

The identified hazards are structured into two different classes for easy allocation and monitoring between system, subsystems and third party organisations where identified:

- a. System boundary or interface hazards. These hazards reside at the interfaces between two subsystems (e.g. between rolling stock and signalling). Management of these types of hazards is the responsibility of the Systems Integration Team on each of the two programmes;
- b. Subsystem level hazards. These type of hazards reside at the project and supplier level and are the responsibility of either the particular project portfolio, project or their key suppliers.

A Hazard Forum has been implemented at the programme level to oversee and address the transfer of hazards between the programme, projects and suppliers and also consider hazards that require effort from multiple projects to facilitate closure. The Hazard Forum is independent from the programme.

An Interdisciplinary Hazard Review Group [IHRG] is formed to address and close-out hazards at project portfolio, project and supplier level. The IHRG oversees and addresses the transfer of hazards between the programme, projects and suppliers and also considers hazards that require effort from multiple projects to facilitate closure. The IHRG is independent from the programme delivery.

The same hazard log management procedure and the hazard log database structure are used across programme and project level. This ensures consistency between the system (programme) hazard log and projects hazard logs.

6. **Use of a common requirements management process**, to support traceability of safety requirements from programme to project and finally to supplier level. Safety Requirements (qualitative and quantitative) are built around the Core Hazards. This is because the only continuous “theme” relevant to the safety argument during the life of the programme of works is a set of the Core Hazards.

Derivation of safety requirements was supported by the following sources:

- a. Railway Legislation and Regulations;
- b. LU Standards;

- c. European and International Standards;
- d. The PPP Service Contract;
- e. The Health and Safety Executive (HSE) Railway Safety Principles and Guidance;
- f. Safety Reports from past accidents in the UK railway industry;
- g. Preliminary Hazard Analysis – Safety requirements have been derived from the review of the mitigation measures identified during the PHA;
- h. Change Safety Analysis - Safety requirements have been derived from the review of the mitigation measures identified during the CSA.

Using the above sources a set of core safety requirements to be met by all project portfolios and suppliers has been established. The safety requirements are generic and include technical and process types. The requirements are applicable at all levels of the programme and for all systems and sub-systems put in to operational use in the SSL and VL railway.

7. **Linkage and consistency between engineering safety cases** (safety arguments and evidences) produced at programme, project and supplier level in order to support the application for Consent to Operate, at key stages of the Upgrade Programmes. The underlying system safety argument is build around a set of safety goals derived from the Core Hazards identified in the System Hazard Log. The programmes make use of the process models to identify boundary interfaces, define and establish the linkages between the safety cases produced at programme, project and supply chain level. Identifying the responsibilities for each identified boundary interface, enables the scope of each safety case to be fixed at programme, project and supply chain level.

Adopting this approach ensures that there is a full coverage of all safety issues arising from the SUP programme works, that there are no gaps in the analysis, but as well, that there is no duplication of effort.

The technical safety report parts of the safety cases are based around the Core Hazards, at project and programme level. Central to demonstrating safety is the use of GSN to outline the safety argument and set out the evidence supporting the case for safety.

In constructing a GSN based safety argument for an overall system safety case, the safety cases of individual sub-systems within the system are used, to supply the evidence. The core hazards are a constant for all parts of the system and for

all configurations of the project, and using them to form the goals of safety justification for each railway system configuration as the project is progressing facilitates the development of consistent and reusable safety arguments. This includes the use of Goal Structuring Notation (GSN), to:

- a. Facilitate identification and management of hierarchy of safety arguments and evidence throughout the programme;
- b. Facilitate the development of railway system safety arguments based on the safety arguments for individual subsystems (developed by projects or suppliers);
- c. Enable the reuse of safety arguments from one stage to another.

7.4 Identification of a set of common core hazards

The Top Events of the LU QRA were used as the starting point for identification of the Core Hazards. Only those QRA Top Events which were believed affected by the changes to the railway within the scope of the upgrade programmes were included in the review.

As already stated the LU QRA are of very narrow scope and in order to confirm the completeness of the core hazards set and its scope it was necessary to identify and fill any gaps (for example workforce related risk and causes which do not result in fatality).

A review was carried out using the following complementary sources of railway risks to complete the list of LU QRA top events:

1. Railway Safety and Standards Board (RSSB) Safety Risk Model;
2. Victoria Line Upgrade (VLU) System Safety Case Core Hazards;
3. Existing SSR System Hazard Log hazard groupings;
4. West Coast Route Modernisation Current Safety Performance of the Railway QRA model.

Each of the QRA Top Events was reviewed for possible omissions highlighted by the other sources. Where appropriate the scope of the Core Hazard mapped to the QRA Top Event, was broadened.

Where there was no suitable existing LU QRA Top Event a new Core Hazard was defined. The Core Hazards were named to maintain an obvious link to any relevant QRA Top Events. The names of Top Events defined in terms of accidents were modified to better reflect the definition of a Hazard e.g. “the potential to cause harm”.

Impacts on	Core Hazards	Definitions
Passenger, Workforce, Member of Public	Potential for collision between trains	This Core Hazard groups Causes, arising from or impacted by the scope of works, which effect the safe separation between trains. This Core Hazard is primarily expected to affect Passengers and Workforce. There is potentially a secondary effect on MOP, were a collision to result in "something hazardous" going beyond the railway boundary.
Passenger, Workforce, Member of Public	Potential for collision with object	This Core Hazard groups Causes, arising from or impacted by the scope of works, which affect the likelihood of objects or animals "find their way" on or near the running railway such that they could make contact with a passing train. This Core Hazard includes those occurrences where the train: - Is incompatible with the structure gauge; - May collide with buffers. This Core Hazard excludes: - Instances of objects on the track causing fires; - Collision with objects which cause derailment. This Core Hazard is primarily expected to affect Passengers and Workforce. There is potentially a secondary effect on MOP, were a collision to result in "something hazardous" going beyond the railway boundary.
Passenger, Workforce, Member of Public	Potential for derailment	This Core Hazard groups Causes, arising from or impacted by the scope of works, where the relationship between the track and the train is compromised such that the train may be derailed. Examples of possible causes include: over-speeding of the train, track degradation outside safe limits, faults at switches and crossings, signalling failures and objects on the line. This Core Hazard is primarily expected to affect Passengers and Workforce. There is potentially a secondary effect on MOP, were a derailment to result in "something hazardous" going beyond the railway boundary.
Passenger, Workforce	People-train incident at the platform interface	This Core Hazard groups Causes, arising from or impacted by the scope of works, which affect people at the platform train interface including, but not restricted too: - Entering or alighting from trains; - Falling off platforms; - Being struck or run over by train (station areas only); - Crossing the lines at station (Where authorised only); - Opening and closing of carriage doors. This Core Hazard excludes Passengers and Workers who deliberately access restricted track areas. These events are within the scope of Unauthorised access to track. This Core Hazard has been extended to also include slip trip and fall Causes arising from or impacted by the changes in platform areas undertaken within the scope of works. This Core Hazard is expected to affect Passengers and Workforce only.
Passenger, Workforce	People-train incident on the train	This Core Hazard groups Causes, arising from or impacted by the scope of works, which affect people on-train due to train movement: This includes, but is not restricted too: - People protruding beyond train gauge during movement; - Loss of train compartment integrity (e.g. Carriage separation, broken windows); - Falls due to train lurching, jerking or rapid deceleration. This Core Hazard excludes a collision with another train, derailment, collision with an object. (All of these are covered by other Core

Impacts on	Core Hazards	Definitions
		Hazards). This Core Hazard is expected to affect Passengers and Workforce only.
Passenger, Workforce, Member of Public	Potential Electrocution	This Core Hazard groups Causes, arising from or impacted by the scope of works, which affect the safe separation of people from live electrical power supplies. This Core Hazard is closely linked to Arcing but is kept separate because the nature of any resulting accident will be different. However the two Core Hazards may be combined together for analysis where it is pragmatic to do so. This Core Hazard may affect Passengers, Workforce and Members of the Public.
Passenger, Workforce, Member of Public	Arcing	This Core Hazard groups Causes, arising from or impacted by the scope of works, which affect arching of electrical power supplies (particular traction power). This Core Hazard is closely linked to Potential Electrocution but is kept separate because the nature of any resulting accident will be different. However the two Core Hazards may be combined together for analysis where it is pragmatic to do so. This Core Hazard may affect Passengers, Workforce and Members of the Public.
Passenger, Workforce	Potential for Train Fire	This Core Hazard groups Causes, arising from or impacted by the scope of works, which affect the potential for on-train fires. This Core Hazard is expected to impact on-train Passengers and Workforce.
Passenger, Workforce, Member of Public	Potential for Station Fire	This Core Hazard groups Causes, arising from or impacted by the scope of works, which affect the potential for station fires. This Core Hazard may affect Passengers, Workforce and Members of the Public.
Passenger, Workforce	Potential for Tracksides Fire	This Core Hazard groups Causes, arising from or impacted by the scope of works, which affect the potential for tracksides fires. For the purposes of this Core Hazard tracksides shall include both open line-side and sub-surface. This Core Hazard may affect Passengers, Workforce and Members of the Public.
Passenger, Workforce	Inadequate ventilation (On train)	This Core Hazard groups Causes, arising from or impacted by the scope of works, which affect the on-train air quality. This Core Hazard excludes fires. This Core Hazard may affect Passengers and Workforce.
Passenger, Workforce, Member of Public	Unauthorised access to track	This Core Hazard groups Causes, arising from or impacted by the scope of works, related to unauthorised access to track. This Core Hazard may affect Passengers, Workforce and Members of the Public.
Workforce	Failure to protect workforce on track from train movements	This Core Hazard groups Causes, arising from or impacted by the scope of works, related to workforce when on or about the track. This includes but is not limited to: • When acting as lookout or hand signaller; • When working on or about the track; • When authorised to walk on the track; • Flying objects or out-of-gauge parts of a train. This Core Hazard will impact on the Workforce only.
Workforce	Workforce	This Core Hazard is intended to encompass all Causes, arising from or

Impacts on	Core Hazards	Definitions
	Occupational Health and Safety	impacted by the scope of works, related to Workforce occupational health and safety which fall outside the scope of all other Core Hazards. This Core Hazard will impact on the Workforce only.
Passenger, Workforce	Potential for flood	This Core Hazard is intended to encompass all Causes, arising from or impacted by the scope of works, relating to the potential for flooding. This Core Hazard may affect Passengers, Workforce and Members of the Public.
Passenger, Workforce, Member of Public	Potential for Structural failure	This Core Hazard is intended to encompass all Causes, arising from or impacted by the scope of works, relating to the failure of structures. This Core Hazard may affect Passengers, Workforce and Members of the Public.
Passenger, Workforce	Evacuation from trains	This Core Hazard is intended to encompass all Causes, arising from or impacted by the scope of works, relating to the evacuation of trains. This Core Hazard may affect Passengers and Workforce.

Table 7-1: SSL Core Hazards definition

7.5 Information gathering, conceptualisation and representation (System Analysis)

To assist the understanding of the interaction between the various systems and elements which comprise the overall system, for each Core Hazard (or a group of Core Hazards), process models have been developed based on the Railway System Physical Architecture and for a relevant Railway Configuration with the aim to:

1. Identify the system boundaries;
2. Identify boundary interfaces and their associated change through migration stages;
3. Identify owners of changes to each boundary interface (i.e. supplier, project or programme);
4. Identify safety functions of the system;
5. Identify the subset of the system relevant to each safety function;
6. Focus attention on the functional interactions between the elements relevant to each safety function;
7. Focus Change Safety Analysis on the elements of the railway that are subject to change;
8. Establish a common reference environment for Safety Analysis and Derivation of Safety Arguments across the programmes;
9. Ensure that there is no duplication of effort in the safety analysis carried out at programme, project and supply chain level.

Process models have been developed with particular focus on the identification and establishment of boundary interfaces and their associated physical, functional or

operational change. Responsibilities for each change to any of the interfaces have been identified and assigned. The scope of the safety analysis is clearly determined by the use of process models, ensuring that there is no duplication of effort in the safety analysis carried out at programme, project and supply chain level.

More importantly, use of the process models provides focus of the analysis on the elements of the railway that are subject to change by the upgrade programme scope of work. A common approach to conceptualisation of the system was adopted in support of the two upgrade programmes, VLU and SSL.

For the purpose of this thesis an example of the process model depicting the same family of “Train accidents” from both programmes has been used. The “Train accidents” comprise collision between trains, collision of trains with buffer stops or movement arresters, derailments, and collision of trains with objects.

The model shown here represents the situation of the first new trains running interspersed with existing trains and the line still being controlled from the existing control room. For simplicity the existing trains and their relation to the track and existing system have not been shown. The safe behaviour of these elements of the system is taken as already proven.

The existing signalling system acts on the track in the sense that it drives the points. It receives information from the track in the form of track circuit inputs and point detection. It also provides energy to lineside signals and receives information in the form of lamp proving.

Specifically for VLU, the new signalling system receives information from the existing signalling system and provides information to control the train via its traction control and braking systems. It should be noted that the element labelled “Signalling System (new)” includes the on-train parts of the signalling system as well as the lineside parts.

The controller controls and monitors the movement of trains via the Service Control Centre system and its links with the signal system, and the line controller and driver can speak via voice communications links. In support of the Victoria Line safety analysis the process models have been developed at the programme/railway system level only. An example from VLU on Figure 7-5 is the process model covering the following core hazards; “Potential for collision between trains”, “Potential for collision with object” and “Potential for derailment” in one process model. An example of interface descriptions for this process model is in Table 7-2 below.

This is because by the time the CSA and ESAP as a process have been implemented the supply chain and project activities have advanced significantly further than the railway system level activities and therefore it was not practicable to develop the hierarchy of process models. Instead, allocation of responsibilities for development of safety arguments has been done through mapping of the VLUP System Architecture interfaces (SCID and O&Idb interfaces) to the supplier's interfaces matrix.

Process Model Ref	IF Ref	Interface (from SCID) Description
TA07	IF0409	09TS Train provides discrete status indications to the Train Operator via the Drivers HMI in the cab.
TA25	IF1352	Track Lubricator provides Lubrication using Mechanical Device (method) via Mechanical (medium) to Trackwork

Table 7-2: VLU Train Movement Accident interfaces description

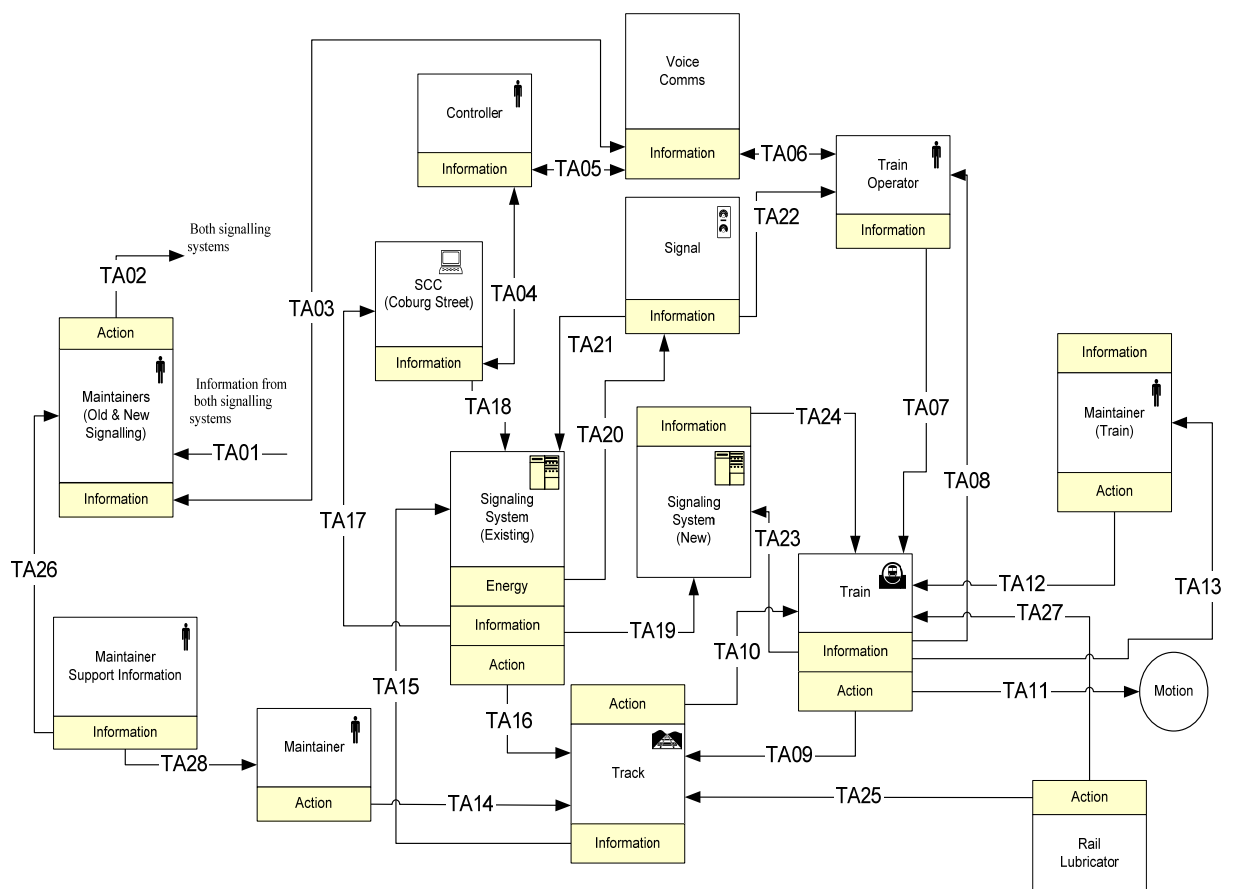


Figure 7-5: VLUP Train Movement Accidents process model

On SSL, the process models have been developed at the programme level initially and subsequently at the project level, resulting in a hierarchy of the process models providing two levels of detail commensurate to the level of detail required to support the engineering safety analysis and management activities.

As depicted by Figure 7-6 the System Level Process model has been further decomposed for each project portfolio scope of works to provide the relevant detail in support of safety analysis at each of the two levels.

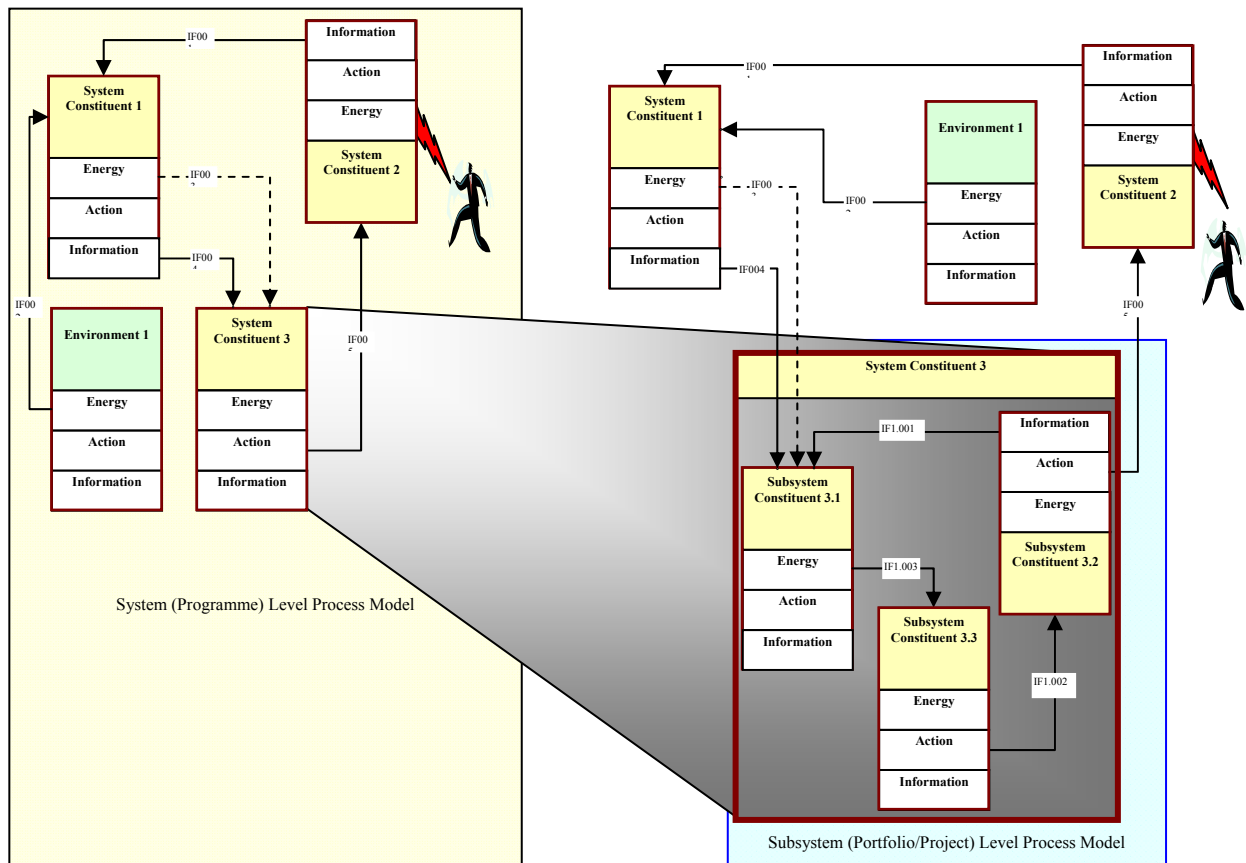


Figure 7-6: Decomposition of process models

An example below, Figure 7-7, represents the system level SSL “Train Movement Accidents” process model.

This process model has been decomposed further into a number of process models for “Immunisation Portfolio”; “Rolling Stock Portfolio”, etc.

In this example, system components indicated by coloured boxes have been decomposed to reflect the scope of the “Immunisation Portfolio” works, see Figure 7-8.

An example of the process models’ interfaces descriptions and hierarchical decomposition is presented in Table 7-3 below.

SSL System level Process Model (Figure 7-7)				
Process Model Interface Id	Upstream Object	Downstream Object	Interface Description	Change
TM07	Current Signalling System	Train Stop	I/L command to actuate train stop movement	Train Stop moved.
Project Portfolio level Process Model (Immunisation Portfolio) (Figure 7-8) with mapping to decomposed interfaces				
TMA29/ TMA65	Current Signalling System object controller	Train Stop via Auxiliary Signal	I/L command to actuate train stop movement	Train Stop moved.
TMA30/ TMA64		Train Stop via Main Signal		

Table 7-3: SSL Train Movement Accident interfaces description

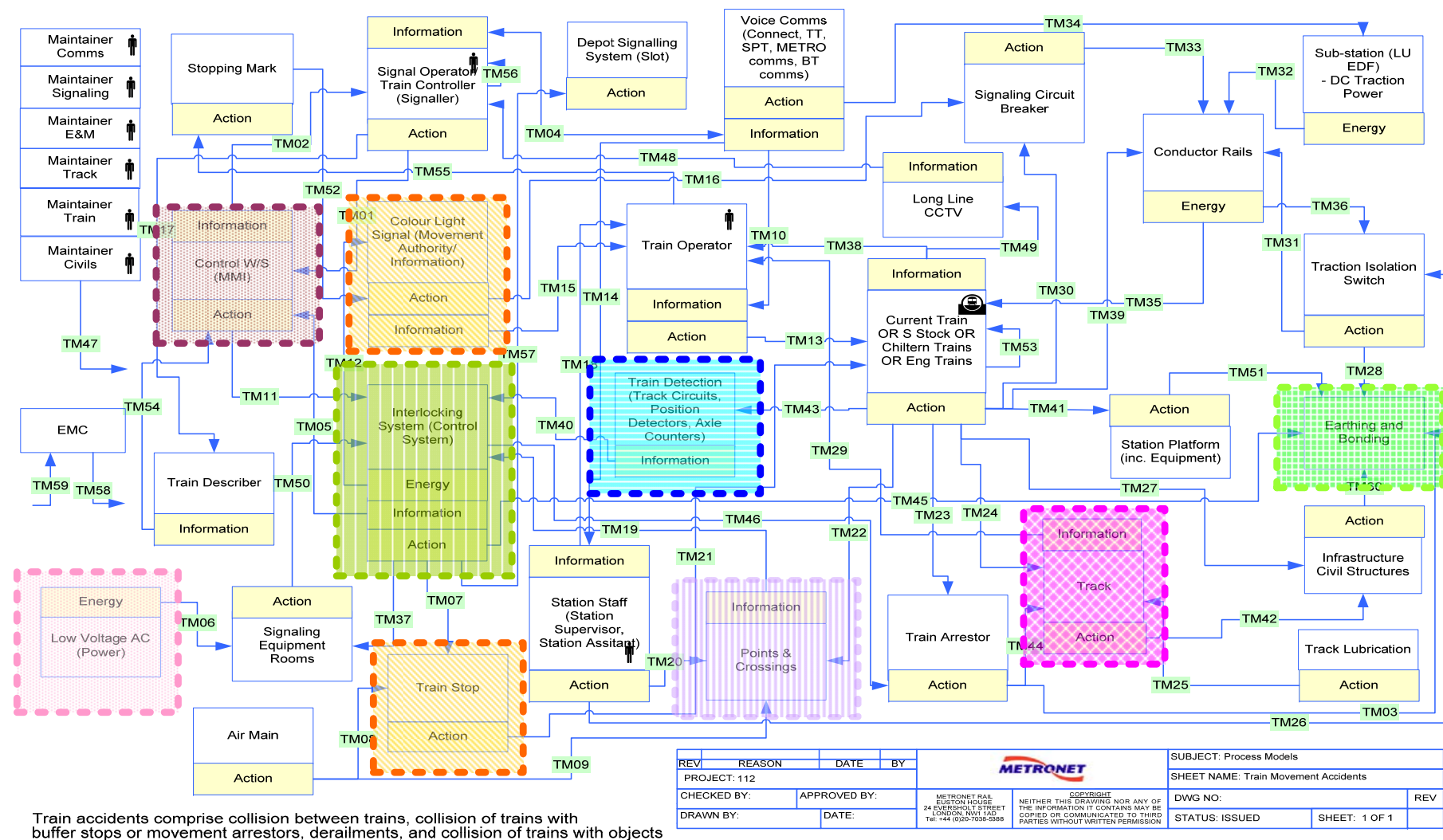


Figure 7-7: SSL System Level “Train Movement Accidents” process model

“Immunisation Portfolio” Level of the “Train Movement Accidents” process model provides more detail relevant to the scope of change to be introduced by this portfolio. On the Figure 7-8, the decomposition of relevant system components is indicated by highlighted boxes.

7.6 Information processing

7.6.1 Change safety Analysis: hazard identification, analysis of causalities and consequences options and impact analysis and risk assessment

As already mentioned in support of further hazard identification, for each Core Hazard a Process Model has been developed and was used to structure the change safety analysis as described earlier. For each interface the ICSA class is identified and recorded, a reference to the relevant core hazard is kept as well as the description of the identified cause. All of the identified causes have been mapped to QRA model elements as well. This activity supported later quantification of some of the safety requirements as detailed later in this thesis.

The comparable risk assessment process was also applied (pre and post implementation of the mitigation) successfully and the results of it used in the safety case arguments as detailed later.

In order to assess the correctness and sufficiency of the identified mitigation measures, the ALARP review process followed the process depicted in Figure 7-9.

It should be noted that the depicted process relies upon the collective expert knowledge and judgement of the assembled workshop participants to determine whether all relevant mitigations have been recorded and make a first-pass judgement on whether any additional mitigations could be reasonably practicable to implement.

To aid the process of assessing the risk of the hazard as a whole as well as adding transparency to the classification process, the author added an additional step to the process depicted in Figure 7-9, the process was applied (by using the same classifications, as in Table 7-4) at the Causal level. It was not always possible to assign a classification at the Causal level and it was recorded where this was the case. The risk acceptability criteria shown in Table 7-5 are not directly applicable when applied at the causal level. For example, it may be acceptable to have a worsening of a minor cause as this might be counter balanced by an improvement in another cause to give no effect on the hazard as a whole. This is particularly relevant at the overlay stages (when new and old trains are to be running at the same time, old trains relying on the old signalling system and new trains on the new DTG-R signalling) as there may be an increase in risk for some causes associated resulting from operational arrangements for trialing (e.g. driver distraction due to additional personnel in cab). Qualitative ranking has been undertaken on a per-hazard basis in accordance with the classification scheme provided in Table 7-4. This ranking was used to confirm

whether the residual risk presented by the hazard, as mitigated by the mitigation measures, is acceptable in accordance with the acceptability matrix presented in Table 7-5 .

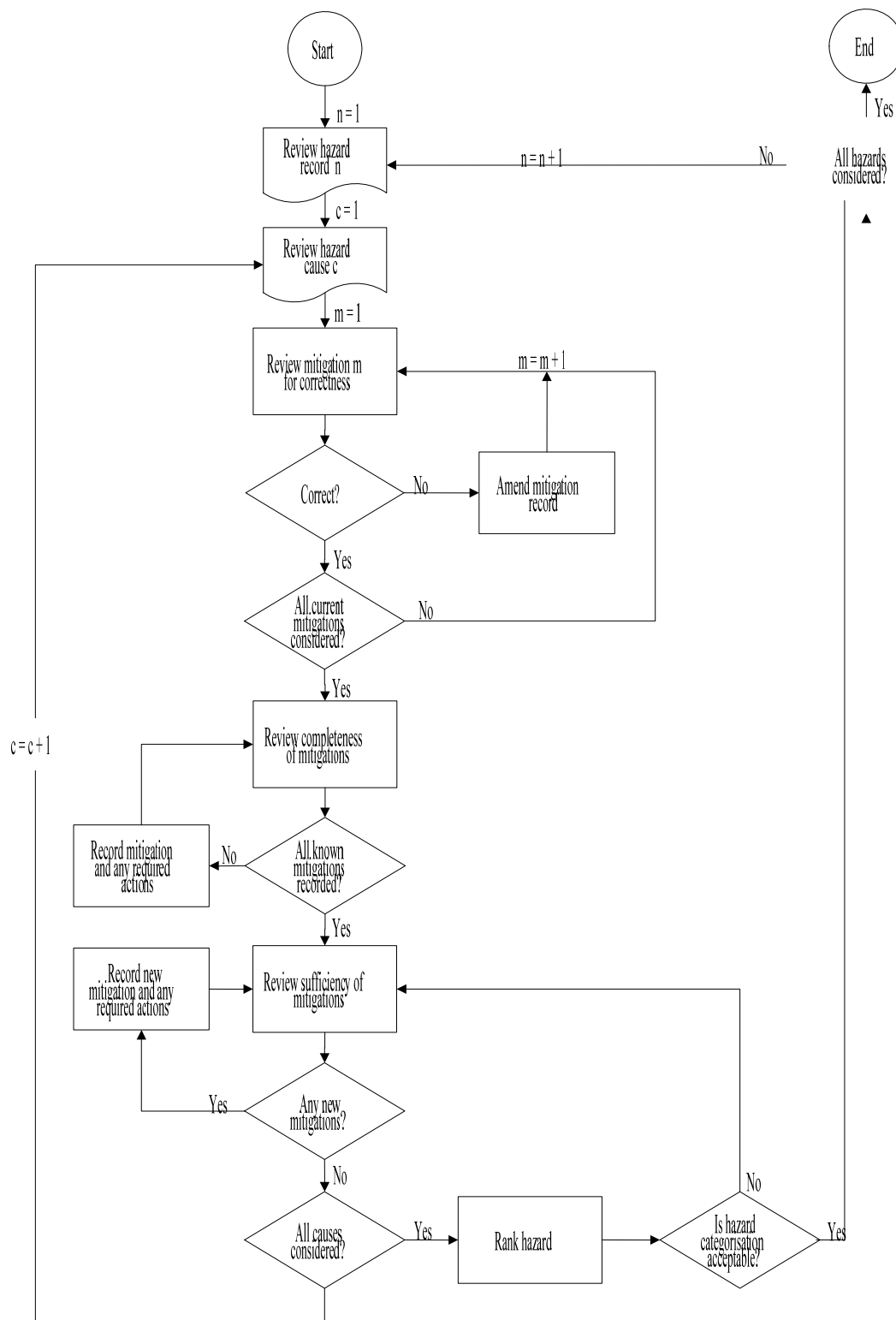


Figure 7-9: ALARP Review Process

	Qualitative Ranking	Definition
Classification 1	BETTER	The risk is assessed as significantly better (lower) than would be achieved with standards or other established authoritative good practice being used
	WORSE	The risk is assessed as significantly worse (higher) than would be achieved with standards or other established authoritative good practice
	COMPARABLE	The risk is assessed as neither Better nor Worse than would be achieved with standards or other established authoritative good practice
Classification 2	MINOR	There are other hazards associated with the VLU Programme that have a risk at least an order of magnitude greater for the group which is exposed to them in the relevant part of the VLU
	MAJOR	There is no other hazard associated with the VLU Programme that has a risk at least an order of magnitude greater

Table 7-4: Qualitative Ranking

	BETTER	COMPARABLE	WORSE
MINOR	Acceptable	Acceptable	Not Acceptable
MAJOR	Acceptable	Further Review	Not Acceptable

Table 7-5: Risk Acceptability

the author used the results of the review, in fact the options and impact analysis, in support of system safety case arguments.

On VLU, process models at the system level were subjected to ICSA and CSA. The analysis was conducted to identify the system level causes, defence/protection measures and consequences related to changing interfaces identified to be between the scopes of work of different suppliers and/or projects. An example of the outcome of the process is presented in Table 7-6 below.

Process Model Ref	ICSA (Change) Class	Core Hazard	Cause		Mitigation		Risk Assessment Classification				Mapping to QRA model	
			Id	Cause Description	Id	Mitigation Description	pre		post		Id	Description
							1	2	1	2		
TA07	1	Collision between trains	1393	Train Operator error - 09TS train operator will be presented with a higher target speed in PM mode in comparison to 67TS. The train operator may over speed when returning to a 67TS and the signalling system will not trip the train at 22mph in Coded Manual.	6543	09 train stock dedicated drivers (if necessary, additional driver briefing).	Comparable	Minor	Comparable	Minor	TO_OVRS_CM	TOp ignores rule and exceeds 22 mph in PM

Process Model Ref	ICSA (Change) Class	Core Hazard	Cause		Mitigation		Risk Assessment Classification				Mapping to QRA model	
			Id	Cause Description	Id	Mitigation Description	pre		post		Id	Description
							1	2	1	2		
TA25	2	Derailment	33459	Insufficient rail lubrication (both T1 and T2 present)	1564	Effective WRI management regime implemented covering lubrication, track inspection and maintenance.	Comparable	Minor	Comparable	Minor	LUBCATN	Poor or inadequate lubrication

Table 7-6: VLU Train Movement Accident-CSA Output Result

On SSL, process models at the system level were subjected to ICSA and CSA first. The system level analysis was conducted to identify system level causes, defence/protection measures and consequences related to changing interfaces identified to be between the scopes of work of project portfolios or where the change is introduced by more than one project portfolio.

Following from that a project portfolio/ subsystem level CSA was conducted, aiming to identify the sub-system or a constituent level causes, defence/protection measures and consequences related to interfaces being changed at this level.

An example of the ICSA/CSA record related to the SSL System Level Analysis is presented in Table 7-7 below.

Process Model Ref	ICSA (Change) Class	Core Hazard	Cause		Mitigation		Risk Assessment Classification				Mapping to QRA model	
			Id	Cause Description	Id	Mitigation Description	pre		post		Id	Description
							1	2	1	2		
TM07	1	Potential Collision Between Trains	247	Loss of Tripcock protection. Trainstop failed in up position while clear aspect is given. (Trainstop fails in up position causing damage to the tripcock when it passes the trainstop at speed, such that the tripcock is then not able to protect the train at a subsequent trainstop)	151	• Signalling protection (Alternate Red Light Circuit driving red lamp) • Signalling Design Process Implemented by competent people; • Testing by Competent people; • Appropriate concessions generated & approved.	Comparable	Minor	Comparable	Minor		

Table 7-7: SSL Train Movement Accident-System Level CSA Output Results

As illustration of the hierarchy of the Change Safety Analysis a change to interface TM07 is taken as an example.

This change, displacement of Train Stops, is being delivered by the Immunisation Portfolio Project. Part of a railway signalling system, a train stop or trip stop (sometimes called a tripper) is a train protection device that automatically stops a train

if it attempts to pass a signal when the signal aspect and operating rules prohibit such movement, or if it attempts to pass at an excessive speed.

As part of the changes implemented by the portfolio, power supply to the signalling system is being upgraded and the train stops are being relocated.

Results of the related CSA are presented in the Table 7-8 below.

Process Model Ref	ICSA (Change) Class	Core Hazard	Cause		Mitigation		Risk Assessment Classification			
			ID	Cause Description	ID	Mitigation Description	pre		post	
							1	2	1	2
TMA29/TMA65 & TMA30/TMA64	1	Collision between trains	008 to 010	Signalling System Unavailable – Loss of supply/incorrect or inadequate supply to signalling equipment: Overall safety risk is considered comparable, some sites are being considered for improvements in availability. Historical discussion around the design methodology. Some changes are recommended however, the project believes that a business case must be generated to enable changes via the ECB.	1620	Recommendation that FRACAS process should be maintained until confidence in failure rates is achieved.	Comparable	Minor	Comparable	Minor
TMA29/TMA65 and TMA30/TMA64	1	Collision between trains	013-026 and 034	RSF, WSF Failures: The overall system EMC has been achieved. Maintenance is being undertaken by the project. Signalling and LVAC training and maintenance is not tested as comparable to having the maintenance organisation undertaking management of maintenance activities. Maintainer will follow the agreed maintenance process. FS2550 Failures (FRACAS reported); Effect is only availability and associated secondary risks (Spads etc). Further discussion on the ballast monitoring regime – no new issues raised.	1564	Training completion and Manual provision must be completed for maintenance staff. Wherever ballast needs to be changed, this has been completed or timescale for change undertaken. Caveat that monitoring is either deemed sufficient for M0 or completed.	Worse	Minor	Comparable	Minor

Table 7-8: SSL Train Movement Accident-Project Portfolio Level CSA Output Results

7.6.2 Restrictions management

It is important to distinguish between the Restrictions, Dependencies and Assumptions. A dependency is an agreement between involved parties that something will be in place before the operation of the change. An assumption is a statement about the system or the rest of the world, including people and organisations with which it will interact, as well as the physical system and the environment. If the above definitions are accepted, both assumptions and dependencies need to be managed and controlled by the project or undertaking but do not necessitate safety analysis. The restrictions however need to be treated in same way as defence/protection measures.

A Restriction or a Caveat is a condition or limitation imposed on the system that must be respected, after the change is put into operation, for the system to remain safe and operable. These can be categorised as:

1. Permanent restrictions – imposed on the system by limits of the operational envelope of the system within its environment;
2. Temporary restrictions – imposed on the system due to interim shortcomings of the system design or implementation.

With increased complexity of the system, in the early stages of a new or a changed system introduction, the number of restrictions is likely to rise; in particular the number of temporary restrictions is likely to be relatively high. On VLUP, as part of the safety analysis in support of the first stage of the project implementation (trial running of one new train in normal operational hours, controlled by the new signalling system) the author invented the following process (Figure 7-10) to identify and analyse all the restrictions. The process is structured as follows:

A. Review and Categorisation: The aim of this is to clearly scope out the boundary of review. This activity is carried out in two steps:

Step 1: Characterisation of inputs into Assumptions, Dependences and Restrictions/Caveats.

Step 2: Identification of causes of identified restrictions and confirmation of completeness and correct mapping to related hazards.

[Example: Causes of Restrictions on the VLU at the stage of the project are typically a fault in the implementation of the software product, a fault in the geographic data or a fault in the product design. For example, Manned Auto Operation, Unimpeded, into platform two is caused by geographic data errors in the map or APRs incorrectly located / programmed at the ramp to the depot. The following hazards have been identified as relevant:

- 1. Inappropriate separation between trains leading to a collision;*
- 2. Possible derailment due to wrong movement of train over unsecured or out of correspondence points, or movement of points under the train;*
- 3. Possible derailment due to over speed;*
- 4. Unwanted Stopping;*
- 5. Electrocution;*
- 6. Collision with object;*
- 7. Possible collision with buffer-stops.*

The top event hazard affected by this issue is ‘Possible collision with another train’ due to excessive RM driving].

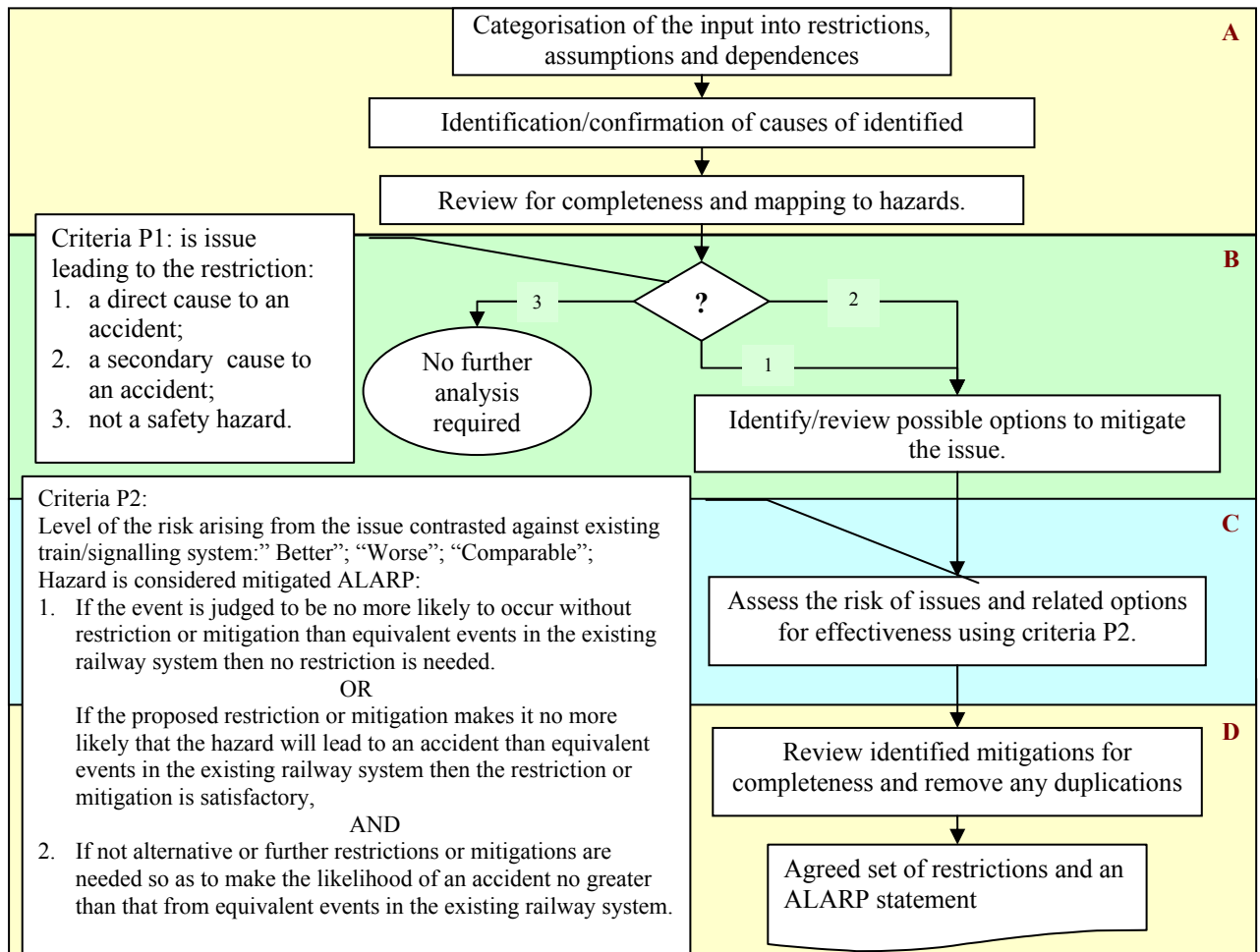


Figure 7-10: Restrictions identification and analysis process

B. Preliminary assessment of impact of causes of restrictions/caveats and identification of Mitigation options:

The aim of this part of the review is to prioritise and carry out identification of options to mitigate identified issues and concerns.

This is carried out in two steps:

Step 1: Review the restrictions applying the criteria P1: Is a cause/issue leading to the restriction:

1. A direct cause to an accident?
2. A secondary cause to an accident?
3. Not safety related?

If a cause/issue does not lead to a safety accident it is recorded and no further action taken.

If a cause/issue is potentially a direct cause of a safety accident it is flagged and subject to further review focussing on these first. If a cause/issue is potentially a secondary cause of a safety accident it is subjected to further review after completing the review of direct causes.

Step 2: Review of existing restrictions and identification of any new mitigation options against safety causes/issues; direct causes first and secondary causes after.

C. Risk assessment and selection of available options:

The aim of this part of the review is to assess the risk of identified causes/issues, effectiveness and practicability of identified mitigations/restrictions and based on that assessment select the mitigations/restrictions to be implemented. This is carried out in three steps:

Step 1: Review the causes/hazards before the restriction is implemented, applying the criteria P2: Is level of the risk arising from the hazard contrasted against existing train/signalling system "Better"; "Worse" or "Comparable"?

Step 2: Review a need for mitigation and where needed the effectiveness of identified restrictions applying the criteria P2.

Hazard is considered mitigated to ALARP:

1. If the event is judged to be no more likely to occur without restriction or mitigation than equivalent events in the existing railway system then no restriction is needed

OR

If the proposed restriction or mitigation makes it no more likely that the hazard will lead to an accident than equivalent events in the existing railway system, then the restriction or mitigation is satisfactory,

AND

2. If no alternative or further restrictions or mitigations are needed to make the likelihood of an accident no greater than that from equivalent events in the existing railway system.

Step 3: Review the causes/hazards assuming that the restrictions are implemented, applying the criteria P2: Is the level of the risk arising from the hazard contrasted against the existing train/signalling system "Better"; "Worse" or "Comparable"?

D. Review of identified mitigations and ALARP argument:

The aim of this, final, stage of the process is to rationalise the output of the workshop and agree conclusion.

An example of the output from the workshop is presented in a Table 7-9 below.

ID	Details of the existing restriction	Source	Related Hazards	Cause		Mitigation Method	Action	Actionee	Risk Assessment	
				Description	Category				Initial	Residual
1	Temporary/Permanent Speed Restrictions (TSR/PSR) imposed by existing means (either maintaining 270 code or recommissioning coasting spots) will not be obeyed by 09TS Maintenance briefing to reinforce existing rules to be published	System design in overlay	Possible derailment due to over speed	Inappropriate maintenance action	Primary	Maintenance and operations briefing to reinforce existing rules on the application of TSRs to be published.	Publish maintenance and operations briefing to reinforce existing rules on the application of TSRs.	Name Surname	Worse	Comparable
3	The testing shall be controlled under an appropriate method statement and test briefing notices. These briefing notices shall include the following: 1. Consideration of how unsafe conditions can arise due to the operation of fault handling devices such as bypass and isolating switches and isolating cocks; 2. How the operator can change the mode of operation of the train borne control system and the pre- and post-change conditions; 3. Details of the driver actions when a train in MA mode stops at a station it should skip; 4. Actions for when the train in MA Mode does not stop accurately at a platform; 5. Actions for when a train in MA mode fails to stop at a station at which it was expected to stop; 6. If, during auto-driving, erratic train movement is experienced, the driver should leave MA Mode change at their earliest opportunity.	Westinghouse testing arrangements restriction	Inappropriate separation between trains leading to a collision Possible derailment due to over speed	ATP fails to intervene when stressed by ATO	Secondary	WRS� train method statement and test briefing notices for T1/T2 Non-Traffic Hours Testing with full reliance on DTG-R	Agreed between all parties that LU rule book / driving manuals and training is sufficient and covers these driver actions - although obviously some of these are not acceptable for traffic / passenger operation and will need to be closed for 2.1 or 2.2. To be agreed with WRS�.	Name Surname	Comparable	Comparable

Table 7-9: Sample of the restrictions analysis outcome

7.6.3 Modelling

The Victoria Line Upgrade and Subsurface Lines Upgrade projects are introducing many changes to the Victoria Line, including new trains and signalling. It is a legal requirement to demonstrate that these changes will not cause the risk of passenger fatality to increase beyond the current levels and is ALARP.

Both projects are being delivered through a series of migrations between defined Configuration States that map to key milestones in the programme thereby changing the risk profile of the railway at each migration stage. To reflect this, the QRA model has been developed for each Configuration State, resulting in a set of risk predictions for passenger fatalities at each stage (defined and analysed in the Interim Safety Performance models).

To ensure that the total risk is kept to an acceptable level, as a minimum a level which is no worse than at present, the QRA models are used to set safety targets for aspects and functions of the systems.

As already mentioned, a set of QRA models developed within the LU was handed over to upgrade projects to support derivation of safety targets and quantification of core safety requirements.

After detailed examination of the LU model it was decided that it was not suitable for defining the current level of risk because:

1. A significant number of logical as well as data errors were identified;
2. The model logic was not fully representative of the current function and operation of the railway;
3. The base data was no longer traceable to a verifiable data source.

The models have been reviewed and updated to provide a Current Safety Performance of the Victoria Line and of the Subsurface Lines (CSPVL and CSPSSL) QRAs.

This revised CSPVL QRAs formed a baseline model of the current railway and are being used to:

1. Confirm the current levels of risk, to set a baseline safety target;
2. Provide a baseline risk model that can be modified to reflect the changes to the railway, for each major migration stage.

Using the CSP models as a starting point, the Interim Safety Performance and the Final Safety Performance models have been developed to define the impact of changes to the railway on the system safety performance.

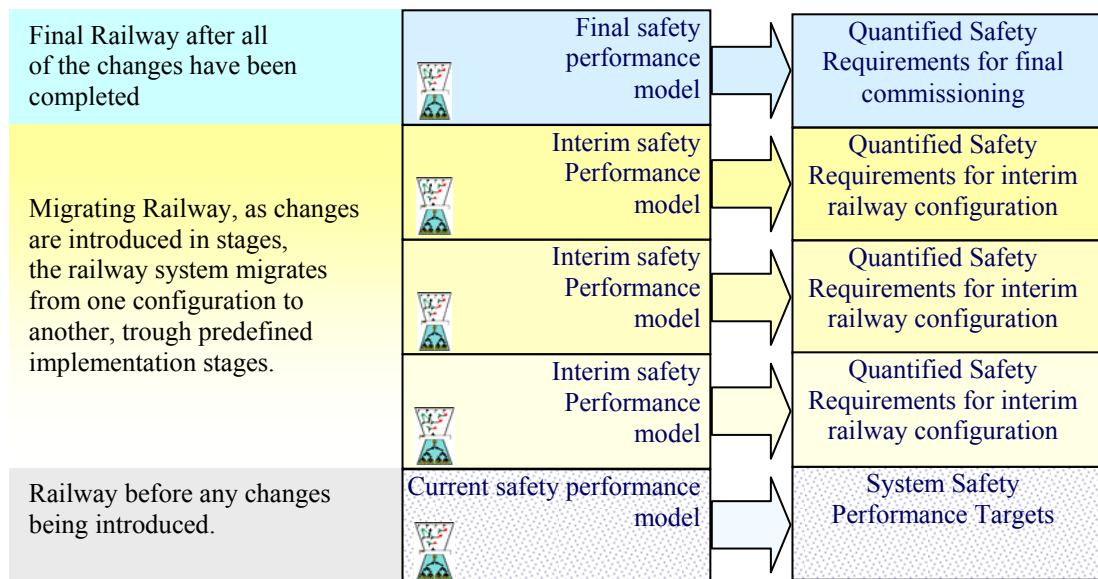


Figure 7-11: Development of QRA models in support of staged project implementation

To achieve this, following activities were carried out:

1. Logic and data of models have been updated to include potential causes of minor and major injuries to all exposed parties (Passengers, Workers and Neighbours);
2. A new loss analysis to predict the injuries and subsequently equivalent fatalities was carried out in some cases;
3. Additionally, in future if the scope changes is altered, it may be necessary to develop further models to include all novel changes.

ISP and FSP series of the QRA models are capable of:

1. Bringing together all the risks from the trains, signalling, track, stations and operators (for modelled hazards only);
2. Integrating with other QRA models (produced by suppliers e.g. Bombardier and Westinghouse) so as to allow for reuse of the data already produced and validated by suppliers;
3. Producing a risk profile given the expected passenger fatality rates resulting from each hazard;
4. Producing a single figure prediction of risk of a fatality to a passenger or worker or neighbour expressed as the risk to the most exposed individual;
5. Calculating the relative contribution (apportionment) of individual causes (interface/subsystem/procedural failures) to the overall risk, originating from each individual hazard.

A regular cross check between the content of the hazard log and the QRA is essential, for each system configuration, to ensure completeness of both sets of analysis during the programmes' lifecycle. In order to track the changes between the different incarnations of the QRA models a change control process has been followed to ensure that each change is transparent and traceable. This process generates a spreadsheet which lists the changes between the two model versions for each model element. This change control register is maintained as a separate spreadsheet for each model and will be updated as new models are produced for each of the project stages.

Scope of the QRA work

The LU 2003 QRA consists of 20 models of the top contributors to safety risk. These are:

- | | |
|---|--------------------------|
| 1. Arcing; | 11. Station fire; |
| 2. Collision Between trains; | 12. Tunnel fire; |
| 3. Collision Hazard (with Object); | 13. Lift fire; |
| 4. Derailment; | 14. Escalator fire; |
| 5. Platform Train Interface- platform; | 15. Unauthorised access; |
| 6. Platform Train Interface- train; | 16. Explosion; |
| 7. Station Area Accident (SAA)-
escalator; | 17. Flood; |
| 8. SAA- lift; | 18. Structural failure; |
| 9. SAA- other; | 19. Power; |
| 10. Train fire; | 20. Ventilation. |

The changes to the railway as a result of the VLU and SSL do not affect all of the models. The models can be split into two groups, models affected by changes and those that are not.

Model	Affected by scope of changes	
	VLU	SSL
Arcing	✓	✓
Collision between trains	✓	✓
Collision with object	✓	✓
Derailment	✓	✓
Passenger Train Interface on train	✓	✓
Passenger Train Interface on platform	✓	✓
Train fire	✓	✓
Tunnel fire	✓	✓

Model	Affected by scope of changes	
	VLU	SSL
Station fire	✓	✓
Unauthorised access	✓	✓
Ventilation	✓	✓
Power		✓
Explosion		
Station Area Accidents - escalator		
Station Area Accidents - lift		
Station Area Accidents - other		
Flood		
Escalator fire		
Structural failure		✓
Lift fire		

Table 7-10: LU 2003 QRAs affected by changes to the railway introduced by VLU and SSL

Only the models affected by scope of change have been subjected to a thorough review and update.

In order to track the changes between the LU 2003 QRA model and the CSP models a change control process has been followed to ensure that each change is transparent and traceable. This process generates a spreadsheet which lists the changes between the two model versions for each model element.

These changes are of the following types:

1. Deleted – The model element has been deleted. This is generally due to a structural change and the change rationale will briefly describe the justification for this change. Full details of the justification for the change are provided;
2. Added - The model element has been added. This is generally due to a structural change and the change rationale will briefly describe the justification for this change. Full details of the justification for the change are provided;
3. Data model or data change – This indicates a change to either the type of data model used and/or the data value used in the model. The rationale for this is described in the appropriate field of the modelling tool;
4. Loss data – This shows where loss data has been revised.

The Data Sources and References in the LU 2003 QRA model were generally not provided whereas in the CSP model a Data Source and Reference has been provided for each event.

This change control register is maintained as a separate spreadsheet for each model and is being updated as new models are produced for each of the stages.

The QRA works in support of the Victoria Line Upgrade have been used in this report as an illustration of works done for both projects.

One of the main reasons for changes is that the Victoria line has some unique features that were not correctly reflected in the LU model:

1. It is all subsurface, consequently there are no embankments, bridges or external environmental effects;
2. It is all twin tunnels, consequently a train cannot collide with a train on the adjacent track except at crossovers;
3. It is all deep tunnel that is mainly straight;
4. There are no curved platforms;
5. There are no speed restrictions due to track curvature, even the points are arranged to be capable of full line speed;
6. The trains are driven automatically by the ATO;
7. The trains are protected by the Safety System, this is a protection system that is completely independent from the ATO train control system;
8. Due to the safety system there is no trip cock protection on the railway. A train driven in SM can pass a signal at danger without being tripped. On an automatic signal a driver can proceed under rule without authority of the signaller, although he should be informed.
9. The train can be driven in three modes:
 - a. Automatic using the ATO called Auto;
 - b. Manually with safety system still providing protection called Coded Manual (CM) (in the event of ATO failure). Speed should be limited to 22mph, but is not enforced;
 - c. Manually at slow speed with no safety system protection called Slow Manual (SM) (in the event of safety system failure). Speed is limited to 10mph and is enforced by the train speed governor.

In addition to above:

1. On all models large numbers of logic gates with no connection to a top gate or an event tree were identified;
2. A number of logical inconsistencies were identified and corrected;
3. None of the data used in the original models was substantiated.

The process of review and acceptance of the revised model logic was as follows:

1. The starting point was LU VL 2003 QRA;
2. The next stage was to identify the known specific characteristics of the VL;
3. The model was then modified to reflect these characteristics. As the model is VL specific if a base even was not applicable it was deleted rather than the data changed to make it have no affect;
4. In order to complete the review process the project organised a final series of workshops and where appropriate experts reviewed and accepted the logic as representative of the current VL;
5. A workshop report was issued to substantiate the changes proposed to the models;
6. Subsequent to the workshop report during the data analysis the need for additional changes to the logic were identified;
7. The additional changes were ratified at a review meeting with the VL Design Authority and Systems Engineering and LU Operations.

Identical process was followed on SSL for review of relevant QRA models. The principle change made was to merge the three QRA models for the SSR lines (the Metropolitan, District, Circle, and Hammersmith & City lines) into one model. This was done recognising that the lines share the same infrastructure for a portion of their length and to simplify the representation of the upgrade.

Summary of Data Update - Methodology

The principle steps for validation of the CSPVL models, representing current configuration of Victoria Line are listed below:

1. Set review scope;
2. Compile list of potential data sources, including scope and coverage;
3. Assess current data set:
 - a. Compile set of new data items (“Obtain”) and identify possible data source;
 - b. Group data items into common sources;
4. Get data for each new data event;
 - a. Define appropriate data model type;

- b. Review source;
- c. Assess uncertainty issues;
- d. Obtain data item(s);
- e. Write rationale, reference and assumptions.

Summary of Data Update - Scope of the Review

The aspects of the model event data which were reviewed are:

- 1. Local or Generic Data Model;
- 2. Data Model Type;
- 3. Rationale;
- 4. Reference.

Summary of Data Update - Data Sources

The data types used in the model were identified in the course of the model data review and are as follows:

- 1. INCA: INCA is the Incident Capture and Analysis database used by LU to capture incidents which occur on the Underground infrastructure. Data has been entered into this database since 1992. Incident data is entered under a particular classification, of which there are 105 different categories. For the data items used in the model the 14 year period between 1992 and 1996 has been used. The aim has been to use incident data from the Victoria Line only. However, in the case that there were few or no incidents of a particular type on the Victoria Line then the search has been extended to then the Bakerloo-Central-Victoria system and, failing that, then the whole Underground system was searched for data. Where this has been done the results have been reviewed to ensure applicability.
- 2. RAM: A number of the event data items in the model are due to equipment failure rates. The data for these items is common with that used for system availability modelling in the VLU project. Data on these failures in use is captured in the CuPID database and it is from this database that the data has been derived.
- 3. Asset Data: There are a small number of asset data items which are needed in the model. However it should be realised that all of the incident data contained in both the INCA and CuPID database is from a system which has a particular set of physical and operational conditions. It is an assumption in the use of these databases that the conditions over the time period that the data are obtained are sufficiently similar to the current system to allow the use of the data.

4. Passenger Occupancy Data: There are two types of passenger occupancy data which are used in the model. The main aspect of passenger occupancy which is required in the event trees is the division between high, medium and low passenger loading.
5. Human Factors: There are a large number of events in the model which are human errors. The probability data for human errors regarding skill and rule-based tasks is general in the range 0.01 to 0.001. While the data provided for human errors is largely presented without justification, it is within this range.
6. Timetable/Number of trains: One of the operational characteristics which affect the risk is the number of trains running on the system. This number has been taken from the signalling availability model and it is one of the operational parameters which describe the system.
7. Judgement: A large number of the failure events in the model are estimates based upon judgement. Where this is the case, operational or engineering expertise has been sought from Metronet or LU competent personnel.

The QRA data set has been assessed against the aspects listed above. As part of this the most appropriate data source for each data item has been identified. The data sources for the different models are shown in Table 7-11 below.

This table lists the number of events for each of the data sources listed above. It can be seen from this table that in addition to the set of data sources listed above there are two additional categories “Model” and “Delete”.

The designation “Model” is used for those elements which are identical to an element in another part of the model or in another model. In this case, the rationale is duplicated and reference is made to the other model element.

The designation “Delete” is made for model elements which are to be deleted. This can be for a number of reasons, as follows:

1. The model element is not used and has no dependencies;
2. The model element is the complement of another model element;
3. The model element is the duplicate of another model element.

Where a model element has been designated “Delete”, the rationale for this has been given.

Model Name	INCA	Judgement	Passenger Occupancy Data	HF	RAM	Clarify	Time table	Asset Data	Model	Delete
Arcing	20	12	0	5	3	0	0	3	45	0
Collision between trains	0	28	0	22	18	2	3	4	48	169
Collision with object	7	0	3	7	10	0	0	2	50	7
Derailment	4	67	0	12	8	1	1	1	107	165
PTI on train	7	13	0	7	6	0	0	0	1	185
PTI Platform	17	37	0	3	2	0	0	0	1	2
Train fire	10	19	8	0	0	0	0	0	5	20
Tunnel fire	10	13	3	24	13	0	0	0	0	9
Station fire	25	20	4	20	14	0	0	2	0	24
Unauthorised access	3	9	0	0	0	2	0	0	0	3

Table 7-11: Model Element Data Sources Overview

Principles for Data Validation in the QRA Model

The development of a model structure is intrinsically linked to the data available to support the model. In general, the level at which the data is available is the level of detail to which the model should be developed.

Sometimes this is in conflict with other model requirements. For example if there is a need to use the model to assess the effect of changes which are at a higher level of detail than the data supports, then there may be a justification for applying subjective judgement techniques to estimate parameters.

In the QRA model, if the model structure is not supported by the data, then an assessment needs to be made as to whether the elements of the structure are required for analysis of system changes. If they are not then the structure should be simplified to the level that the data supports.

Loss data

The loss data for each consequence was checked for validity both in the context of the specific model and in the context of the model as a whole. The basis for this checking was other industry models such as the Railway Standards and Safety Board Safety Risk Model and the West Coast Main Line Current Safety Performance Model.

However it should be noted that as these models are for heavy rail only, the loss data could not be directly compared in many cases and historical data was used as a reference point, including a set of incident data for train accidents in tunnels.

The overall approach was to leave the loss data unchanged from the LU 2003 QRA model unless a specific discrepancy was noted.

The loss data will be further reviewed if affected by changes in the VLU or SSL.

Summary of the Initial Findings

The first finding of the data review was that information regarding the data (the rationale) was not available in a single source.

Instead, descriptions to different levels of detail were contained in both the FT+ model and in a number of other reports. Hence the first task was to gather all of the information in a single source so that it could be reviewed. This was done by exporting all of the FT+ models events as Excel spreadsheets and importing into these all of the descriptions from the other reports.

These spreadsheets formed the basis for the model review with reference to the model structures in FT+ where required. It is desirable that all information regarding the event data (excluding the change history) should be held in the FT+ model. However there are restrictions in terms of the number of notes fields available (8) and the size of those fields (255 characters). Also some of these fields may be required for description and assumptions regarding the logic.

Hence the available fields have been used as follows:

1. Reference: Data source reference including any spatial or temporal aspects;
2. Data source: A description of how the data items were derived from the data source;
3. Planned Maintenance;
4. Assumptions

Where addition information was required which did not fit in these 4 fields, then reference has been made as to where it can be found either in the Data Gathering and Validation report or the data change register/database which exists outside of the model.

Results

Having validated the CSPVL model data set, the next task was then to import all of the data into the FT+ models so that the models could be run and the overall results checked against the existing LU models. An example of the results for Collision with Trains model is presented and discussed below. The LU model divides collision between trains into Fast, Medium or Slow and Head on Fast or Slow. The causes are mainly attributed to signalling wrong side failures or the driver passing a signal at danger in SM or reversing.

The major changes of the QRA logic, in the CSPVL model, were:

1. Failures in Coded Manual mode are added. This is specific feature of the Victoria line signalling ;
2. The interlocking setting conflicting routes is added. This base event was missing from the original QRA model;
3. The train driven in SM following safety system failure is added. This is specific feature of the Victoria line signalling;
4. The modelling of Automatic Train Operation related failure is improved.

In terms of data, the main changes made are as follows:

1. The LU 2003 QRA passenger train loadings have been reviewed and revised. In the LU 2003 QRA model, High loading was estimated to occur 0.1% of the time (i.e. one minute of each operational day), medium loading 2% of the time and low loading 97.9% of the time. These have been revised to: high loading 10%, medium loading 16%, low loading 74%;
2. The LU 2003 QRA model assumed complete segregation of tracks, whereas the CSPVL model has taken into account the two crossovers on the VL.

Following are Risk Results from the updated CSPVL Collision with Trains model.

CSPVL	LU 2003 QRA
0.067	0.062

Table 7-12: Total Risk (fatalities/yr)

Original Model LU 2003 QRA Model		Updated CSPVL Model	
Event Description	Frequency	Event Description	Frequency
Fast collision between trains	1.39E-02	Fast collision between trains	1.23E-04
Head on collision between trains	0.00E+00	Head on collision between trains	3.52E-02
Slow speed head on collision between trains	4.18E-04	Medium Speed collision	4.43E-03
Medium speed collision between trains	1.83E-03	Slow speed collision of two trains	4.32E-08
Slow speed collision between trains	3.08E-03		
Total	1.92E-02	Total	3.98E-02

Table 7-13: Comparison of Initiating event frequencies

At the level of initiating event, the CSPVL model calculates the frequency to be approximately 50% less than that calculated by the LU 2003 QRA model. Given the rarity of this type of event this is degree of variation is not significant.

In the event tree the risk calculated by the CSPVL model is slightly greater that that calculated by the LU 2003 QRA model.

While there is a small effect from the inclusion of head on and subsequent collisions in the CSPVL model, this difference is almost entirely due to the different apportionment to passenger loading levels which has been explained and justified above.

Conclusions from the review of the baseline QRA and definition of Tolerable Hazards' Rates

A summary of the risk results for all of the 10 models updated for the Victoria Line is presented below.

Model Name	CSPVL Risk	% of VL Total	LU VL 2003 QRA Risk	% of LU VL 2003 QRA Total	% change between CSPVL and LU VL 2003 QRA
1. Arcing	1.86E-03	0.30%	2.09E-03	0.22%	-11%
2. Collision between trains	0.068	10.86%	6.19E-02	6.46%	10%
3. Collision with object	3.25E-03	0.52%	1.90E-03	0.20%	71%
4. Derailment	0.0388	6.20%	5.95E-02	6.21%	-35%
5. PTI on train	0.138	22.04%	4.78E-01	49.91%	-71%
6. PTI platform	0.331	52.86%	2.25E-01	23.49%	47%
7. Train fire	0.0138	2.20%	8.48E-02	8.85%	-84%
8. Tunnel fire	2.10E-05	0.00%	1.12E-03	0.12%	-98%
9. Station fire	4.58E-03	0.73%	9.54E-05	0.01%	4701%
10. Unauthorised access	0.0269	4.30%	0.0433	4.52%	-38%
Total	6.26E-01		9.58E-01		-35%

Table 7-14: Summary of Risk results

It can be seen that there is a decrease in risk of 35% over the LU 2003 QRA total for these 10 models. There have been many changes between the two sets of models, both structurally and in terms of data. The principle reasons for the differences are as follows:

1. A number of changes in model structure, data and loss apportionment have contributed to differences in the risk in the CSPVL Derailment, Train Collision and Collision models as compared to the LU 2003 QRA models;
2. The risk due to PTI on Train has reduced by 71% in the CSPVL model as a result of a better alignment with INCA data. As this model constituted 50% of the LU 2003 QRA total risk for these 10 models, this reduction is the main contributor to the decrease in the total.
3. All of the fire models have changed significantly, though they are not major contributors to the overall risk. This is due to changes in model structure to enable the models to be closely based upon incident data.

All of the above comparisons have been made against the LU 2003 QRA, as due to the low incidence of fatality on the LU network as a whole (averaging 4 per annum, excluding suicide), it is not possible to conduct comparisons at any level of detail.

This is consistent with the low frequencies of the initiating events which are in general of the order of one in one hundred or less. It should be remembered that the aim of this validation exercise is to give a baseline set of models which is representative of the current Victoria Line on which the operational and infrastructure changes of the different stages of the VLU can be imposed and effects on safety assessed.

On this basis the conclusion was reached that this updated set of the CSP QRA models is a suitable representation of the hazards on the VL. As such it provides a suitable baseline which was used to set a baseline safety target, Tolerable Hazard Rates (THRs). From that, the total contribution to overall risk, for each Core Hazard, from failures of the new signalling equipment was calculated. Only apportionment to the new signalling system and to rolling stock was calculated, since other changes to the Victoria Line are conventional changes and no new or novel equipment is being used.

Top Event	Risk (fat./yr) THR	Apportionment to Signalling (contribution)	Notes
1. Arcing	1.86E-03	0.00%	
2. Collision between trains	6.81E-02	1.28%	A safety factor of 2x has been applied to account for signalling sub-system failures which may not have been modelled in detail in the Current Safety Performance-Victoria Line (Baseline) mode.
3. Collision with object	3.25E-03	0.00%	Signalling contribution is non-zero but negligible.
4. Derailment	3.88E-02	4.45%	
5. PTI on train	1.38E-01	0.00%	
6. PTI platform	3.31E-01	0.00%	
7. Train fire	1.38E-02	0.00%	
8. Tunnel fire	2.10E-05	0.00%	
9. Station fire	4.58E-03	0.00%	
10. Unauthorised access	2.69E-02	0.00%	

Table 7-15: Victoria line THRs

The above data (apportionment) were calculated by identifying all of the events in the models relevant to signalling and conducting an analysis of the cut set to calculate the contribution to the overall individual risk for that Core Hazard.

The aim of this analysis was to allow the supplier of the signalling system to consider the cost, for each top event, of an “effort” to reduce the risk for an individual hazard from (say) 1E-9/hr to 1E-10/hr, and if the predicted costs are comparatively small, to

justify a general statement, that further cost benefit analysis is not necessary for each top event.

The ALARP argument was produced (in line with LU Standard 2-05101-101) using a value of £1.4 million as the value of avoiding a fatality (VAF) to calculate the safety benefit associated with a measure. A factor of 3 was applied to the safety benefit to assess whether the cost of a measure is grossly disproportionate to the achieved safety benefit.

However, this did not preclude analysis (quantitative or qualitative) of specific issues where it was required.

Development of Interim Safety Performance Models

The overall railway level safety requirements are that:

1. The levels of risk after the change shall be ALARP, and
2. No greater than the current level of risk.

For the VLU project, the update of the QRA reflecting the system changes implemented as part of the first system configuration (referred to as V2.1), has been used in support of the safety argument presented in the System Safety Case (elaborated later in this thesis). This QRA model is referred to as ISP V2.1 (Interim Safety Performance for migration stage/system configuration V2.1). This update included a review of the VL QRA model against the models developed by the rolling stock and signalling system suppliers to ensure that the models are sufficiently consistent to test if the tolerable hazard rates and other targets used by the suppliers are suitable to reduce risk to an acceptable level. The ISP V2.1 QRA model has been used to assess the anticipated level of risk at the railway system configuration compared to the baseline level as estimated by the CSPVL Baseline model.

As part of the system configuration V2.1 an extra pathway in off-peak hours (after 20:30) on which to test the new system, was created (the new train did not carry any passengers). Hence the modelling approach was to change the baseline model to represent the risk posed by the new train on this single train path, the total risk is the risk from the baseline model (which is unchanged as V2.1 does not alter the existing system nor the existing service) together with the risk from the new ISP V2.1 model (representing the risk from a new, overlaid system and the additional train path). It should be noted that as the QRA models risks to passengers only the effect on risk to the drivers, testers or maintainers has not been addressed in these models. These risks have been assessed separately using the comparative methodology described earlier.

As a result of this approach, for each configuration of the system architecture for which a System Safety Case is being prepared, a representative QRA model will consist of a Baseline model with altered data to reflect the changes, and the model reflecting the logic and data changes provided by improvements or new system components such as new trains. This approach results in there being two risk models to model the overall risk of V2.1 operation: one which models the existing system and one which models the new system. This allows each model to represent the different functionality of the old and new system and any interfaces between the two to be explicitly represented.

As more new trains are introduced to replace the existing rolling stock, the initiator data in each model is changed accordingly so that the risk from each system can be calculated at each migration stage. When all of the old rolling stock is replaced by the new train, then the existing system risk will be zero (as the initiator data will be zero) and all of the risk will reside with the new system. This can be represented by the following formula:

$$R_{totalVx}^{ISP} = R_{Vx}^{CSP} + R_{newVx}^{ISP}$$

Where

$R_{totalVx}^{ISP}$ Total risk for migration stage Vx (fatalities/yr);

R_{Vx}^{CSP} Risk from operating with existing signalling and rolling stock for migration stage Vx (fatalities/yr);

R_{newVx}^{ISP} Risk from operating with new signalling and rolling stock for migration stage Vx (fatalities/yr).

The first task in the upgrade of the CSPVL models to represent ISP V2.1 was to review each of the ten hazard models relevant to the VLU to assess if and how these are affected by the changes implemented in phase V2.1. The following Table 1 presents the results of this assessment.

Top event	Effect on passenger risk for V2.1 new train service	Changes to risk model
(potential for) Collision with trains	As it is assumed that the risk from collision between 67TS remains unchanged, the new risk is that a failure of the T2 train control and protection causes a collision with a 67TS resulting in passenger fatalities on the 67TS train. It is assumed that the new signalling system will not negatively affect the wrong side failure rate of the existing signalling system.	The baseline train collision model has been altered to represent the risk of collision due to failure of the new signalling and/or train. All initiator data has been changed to represent the operation of a single train path for 4 hours per day. Exposure data in terms of train loading (of the second as the T2 is not carrying any passengers) has been modified to represent operation in off-peak hours only. These changes result in a new ISP _{V2.1} model.

Top event	Effect on passenger risk for V2.1 new train service	Changes to risk model
(potential for) Collision with Object	The risk from the Collision Hazard for the 67TS remains unchanged. The only new risk is that the object derails the train and subsequent to derailment the T2 train is hit by a train carrying passengers	For T2 the consequence analysis has been changed to remove fatalities resulting from derailment with no subsequent collision and where subsequent collisions occur to only include the effects of loading of the 67TS (rather than combined loading) The causes for objects on the track remain unchanged. All initiator data has been changed to represent the operation of a single train path for 4 hours per day. Exposure data in terms of train loading (for a subsequent collision, as the T2 is not carrying any passengers) has been modified to represent operation in off-peak hours only. These changes result in a new ISP _{V2.1} model.
(potential for) Derailment	The only new risk is that T2 derails and is subsequently hit by a 67TS.	The 67TS risks remain unchanged. The baseling model has been developed to exclude fatalities from derailment without subsequent collision and in the event of subsequent collision only includes the 67TS loading. The causes of derailment (the fault trees) have been changed to take account of the new signalling and trains. These changes result in a new ISP _{V2.1} model.

Table 7-16: Sample of QRA changes relevant to ISP

Having identified where changes to the risk models were required, a more detailed review of each model was conducted to identify specific gates and base events concerning aspects of rolling stock and signalling for which a mapping to the rolling stock and signalling fault trees was sought. The V2.1 risk assessment has modified the Victoria Line baseline QRA models to take account of the following:

1. The train brake and traction and control failure rates as defined in the supplier's model (BT VLU Vehicle level Fault Trees), have been used in the ISP_{V2.1} model;
2. The DTG-R signalling system failure rates as defined in supplier's model (WRSL Signalling and Train Control System Preliminary Fault Tree Hazard Analysis), have been used in the ISP_{V2.1} model;
3. The supplier's model (BT VLU Vehicle level Fault Trees) did not include failure rates for the mechanical or structural elements, e.g. bogies, wheels, suspension etc. Where rates were included in the model the figures from the baseline were used on the grounds that the design was based upon standards and best practice so the rates should be similar to those achieved on the 67TS;
4. The use of Connect digital radio to replace the cab radio and allow the train

operator to communicate directly with other operators as required is included in the $ISP_{V2.1}$ models;

5. The V2.1 risk analysis assumes that the T2 train is used for a year (all rates are per year and all Initiators are events per year). The total risk has been scaled for the relative proportion of usage of T2 and 67TS trains in each of the different phases. In V2.1 only one train path in off peak hours (after 20:30) is being created for the T2 train;
6. The V2.1 loss analysis has been adjusted for the fact that one of the trains has no passengers. Also T2 collisions can only occur at off peak low loading all losses associated with high or medium loading have been set to zero;
7. The V2.1 models, model the risk from the T2 train operating without passengers on the extra path which has been created in off-peak hours. The risk from this operation has been added to that from the Baseline model to obtain the total risk from the V2.1 operation. Hence the data changes have been of two types: the changed failure data for the new rolling stock and signalling systems and the changed exposure data in terms of number of train movements;
8. The changed data for the new rolling stock and signalling systems has been obtained from the suppliers fault tree models. In some cases these values have been set as requirements which the systems must be shown to meet. It is assumed that the supplier's assurances cases will demonstrate how these targets or requirements will be met and testing in engineering hours will highlight any potential issues. Any requirements or targets not achieved will have to be resolved before the new train goes into service in passenger hours.

The assessment of the impact of system changes on its' safety performance using ISP QRA

A summary of the changes made to the models to represent V2.1 and a comparison of the $R_{totalV2.1}^{ISP}$ risk against the CSPVL baseline risk is presented below.

Model Name	R_{Vx}^{CSP}	$R_{totalV2.1}^{ISP}$	% change from CSPVL Baseline
1. Arcing	1.860E-03	1.860E-03	0.000%
2. Collision between trains	6.800E-02	6.800E-02	0.001%
3. Collision with object	3.250E-03	3.266E-03	0.490%
4. Derailment	3.880E-02	3.882E-02	0.054%
5. PTI on train	1.380E-01	1.380E-01	0.000%
6. PTI platform	3.310E-01	3.310E-01	0.000%
7. Train fire	1.380E-02	1.380E-02	0.000%
8. Tunnel fire	2.100E-05	2.100E-05	0.000%
9. Station fire	3.860E-03	3.870E-03	0.258%

Model Name	R_{Vx}^{CSP}	$R_{totalV\ 2.1}^{ISP}$	% change from CSPVL Baseline
10. Unauthorised access	2.69E-02	2.693E-02	0.100%
Total	6.255E-01	6.255E-01	

Table 7-17: Summary of Risk results

As the change in V2.1 was to introduce a new train path, an increase in risk over the baseline is expected. However it can be seen that this increase is negligible or zero for the 10 hazards affected by the VLU. The results of this analysis have been used in support of the safety argument within the safety case, as detailed later.

Apportionment and confirmation of safety targets

As already elaborated, the baseline QRA model (CSPVL and CSPSSL) define the Tolerable Hazard Rates (THR) for the Victoria Line and Subsurface Lines railway systems, for each of the core hazards. In order to apportion the THR to specific constituents of the system, for which a quantified target (or a failure rate) is required in support of safety requirements quantification, further analysis has been done as follows:

1. The system elements affected by the changes brought about through implementation of VLU and SSL project scopes have been identified and the changes classified as per each subsystem (signalling, rolling stock, power, etc);
2. The impact of these changes on the QRA model has been analysed and scoped;
3. The QRA elements have been classified to enable apportionment;
4. Contribution to overall risk for each of the core hazards has been calculated.

For example, for Victoria Line, the result of this analysis, an analysis of the signalling contribution to risk as calculated from the CSPVL QRA model are as in the Table 7-18 below.

Top Event	Risk (fat./yr)	Signalling Contribution	Notes
1. Arcing	1.86E-03	0.00%	
2. Collision between trains	6.81E-02	1.28%	A safety factor of 2x has been applied to account for signalling sub-system failures which may not have been modelled in detail in the CSPVL model
3. Collision with object	3.25E-03	0.00%	Signalling contribution is non-zero but negligible.
4. Derailment	3.88E-02	4.45%	
5. PTI on train	1.38E-01	0.00%	
6. PTI platform	3.31E-01	0.00%	Signalling contribution is non-zero but negligible.
7. Train fire	1.38E-02	0.00%	
8. Tunnel fire	2.10E-05	0.00%	
9. Station fire	4.58E-03	0.00%	
10. Unauthorised access	2.69E-02	0.00%	

Table 7-18: An analysis of the signalling contribution to risk as calculated from the CSPVL

These data were calculated by identifying all of the events in the models relevant to signalling and conducting an analysis of the cut set to calculate the contribution to the overall individual risk for that hazard.

A similar exercise was completed in support of the Subsurface Lines Upgrade Programme, in particular in support of the quantification of safety requirements intended for tendering for a new signalling system. More detail and examples of this work are in the following section.

On the Victoria Line project, specifically, for signalling and rolling stock subsystems, the suppliers have developed their own safety targets early in the life cycle of the project, prior to development of the overall London Underground safety targets described earlier. Therefore, the only pragmatic solution was to use the developed ISPVL and FSPVL models to confirm that the solution being provided by the supply chain will deliver, as a minimum, safety performance commensurate with the safety performance of the existing subsystems (signalling and rolling stock).

This was done by substitution of relevant parts of logic or data in the CSPVL model to derive ISPVL model and results are presented in Table 7-17.

As result of this work the supply chain safety targets have been accepted.

Furthermore, this information was used to support the supply chain's ALARP review, allowing consideration of how much it will cost for each top event to reduce the risk for an individual hazard from (say) $1\text{E-}9/\text{hr}$ to $1\text{E-}10/\text{hr}$ and if the predicted costs are disproportionate, to justify a general statement, that detailed cost benefit analysis is not necessary for each top event.

The ALARP argument was produced in line with LU Standard which requires that "a value of £1.4 million is used as the value of avoiding a fatality (VAF) to calculate the safety benefit associated with a measure".

A factor of 3 was applied to the safety benefit to assess whether the cost of a measure is grossly disproportionate to the safety benefit achieved.

7.7 Derivation of safety requirements

As already mentioned earlier, safety requirements can be grouped into two categories:

1. Requirements related to compliance with standards and good practice;
2. Specific system safety performance related requirements.

Requirements related to compliance with standards and good practice are relatively easy to identify and on both SSL and VLUP these were identified by the safety team at early stages of the lifecycle.

The second category, specific system safety performance requirements were elicited through the review of mitigations/protection measures in the hazard log. Those mitigations/protection measures that are related to novel equipment or new process or novel environment within which the conventional equipment or a process is to operate were converted into safety requirements. Those safety requirements that are related to novel equipment were further analysed to facilitate the representation of these in the QRA either as base events or logical gates.

Quantified targets were set upon these requirements. Table 7-19 presents an example of the VLUP safety requirements, with 4 quantified requirements (R00001, 25, 26 & 28) in italic font.

Requirement No.	Description
R00001	The CSPVL QRA shows that to meet the overall goal of achieving risk levels proportionate to those in the overall LU risk model the risk due to collision between trains on the Victoria Line should be not greater than $6.81 \cdot 10^{-2}$ fatalities per year.
R00005	All equipment specified shall be compliant with new EMI/EMC legislation.
R00006	All trainborne and trackside communications equipment shall not be susceptible to trainborne EMI/Regenerative braking.
R00007	Configuration control of Automatic Train Protection (ATP) map data shall be enforced throughout the life cycle of the system (Metronet asset performance issue).
R00008	Configuration control of trackside and train borne ATP data shall be implemented.
R00009	Configuration management of track capability data linked to signalling data shall be implemented.
R00011	Design of the track circuit configuration shall be compatible with 09TS (e.g. straddle existing short depot track circuits).
R00012	Door alarms to be fitted on Signalling Equipment Room (SER).
R00019	Mobile and portable radio equipment shall be banned from SERs (and other areas) if analysis shows this to be necessary
R00022	Operational procedures for safety critical communication between the train operator and the controller shall be reviewed and updated and appropriate training provided.
R00023	Power and signalling cables shall be sufficiently separated electromagnetically to comply with Standards.
<i>R00025</i>	<i>The likelihood that ATP Movement Authority is exceeded in Protected Manual mode of operation shall not be greater than $7.67E-8$ to ensure the same level of safety performance as today</i>
<i>R00026</i>	<i>The likelihood that the Automatic Train Operation (ATO) system attempts to exceed the stopping point shall not be greater than $2.44E-5$ to ensure the same level of safety performance as today</i>
<i>R00028</i>	<i>The likelihood of the Emergency Brake being unavailable on two or more cars shall not be greater than $1.49E-7$ to ensure the same level of safety performance as today</i>
R00042	The overlay of the new signalling system must not affect the operation of the existing signalling system
R00046	The track lubrication system shall be designed to ensure that relevant standards have been adhered to and that the performance of the railway targets can be met.
R00047	Trainborne EMI/Regenerative braking shall not degrade or incapacitate train borne or trackside communications equipment.
R00049	Validation of data shall be carried out for each change.

Table 7-19: Examples of Victoria Line related Safety Requirements

7.8 Construction of the safety arguments logical network – Safety Justification & Case

In support of both projects, VLUP and SSL, the safety justifications and safety cases were produced (and are still being produced), as an outcome of the above described safety management process. As an illustration of this, one example of a development of the safety justification and a safety case from VLUP and an example of the hierarchy of safety cases from SSL will be presented in this section.

As already outlined the process models inform the change safety analysis (CSA). The output of the CSA feeds the hazard log and the identification of the safety requirements, as illustrated by Figure 7-12 below.

This information is used as a base for further safety analysis, identification and assessment of effectiveness of the protection measures and safety requirements and construction of the safety fact net.

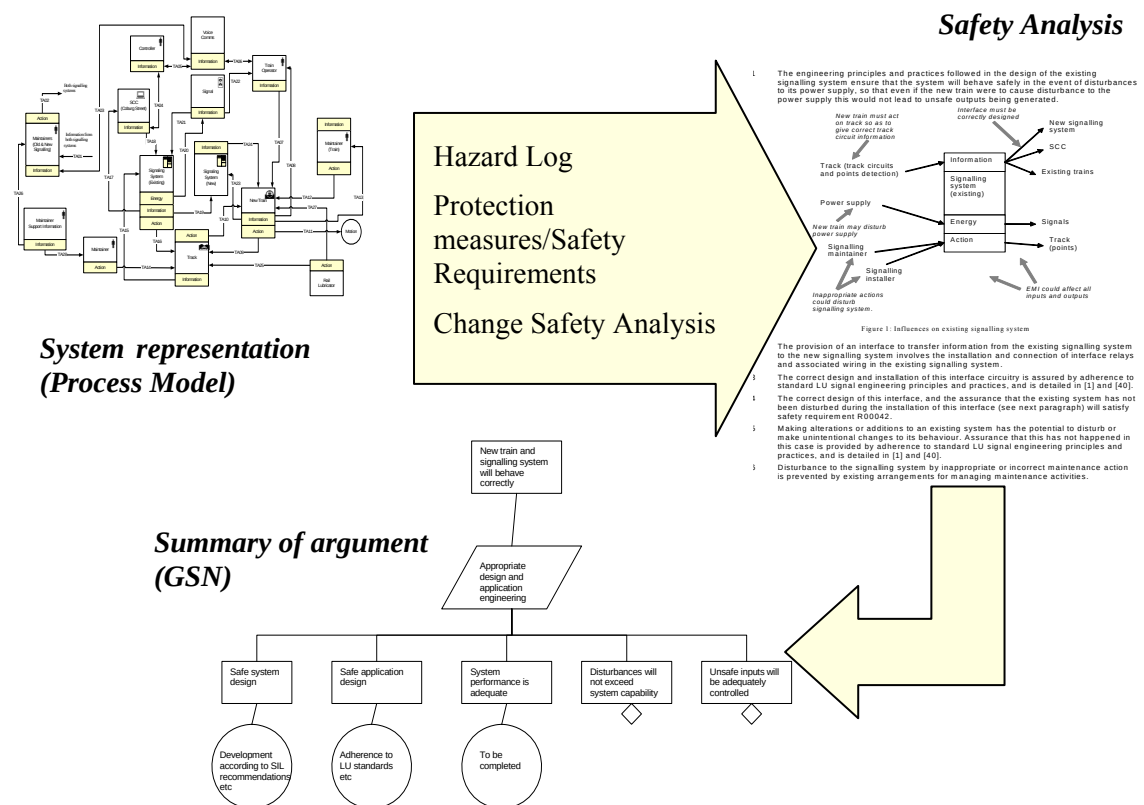


Figure 7-12: Development of Safety Arguments

7.8.1 Safety Justification

Usually, testing is the first life cycle stage that calls for a safety argument to be produced in support of carrying the testing or a trial operation. Production of such a “Safety Justification” is the first step towards production of the safety case. Most often, the process for derivation of the “Safety Justification” is exactly the same as the process for production of the safety case. However, the overall delivered safety

performance of the changed system, to enable the testing, is most often less onerous than in case of the system being fully commissioned. This is due to the fact that the testing is done in controlled environment and it is possible to rigorously enforce many more operational controls that must be in place to compensate the unproven or still unsatisfactory safety performance of the system.

The safety justification is based around the proof of adequate management of hazards, restrictions and incident control and management and an argument that these three key elements of the safety management system deliver safe system for testing. As an example from VLUP, a safety justification that was produced in support of the testing of the new train and the new signalling system in non-traffic hours is presented on Figure 7-13 below. This particular testing was carried out under operational control of London Underground whilst the train-signalling system was delivered by the supply chain, including the proof of safety of the technical solution. The author structured the system safety justification around the three lines of reasoning, mentioned above, and an additional justification of purely technical safety performance of the subsystem delivered by the supply chain, as follows (the structure of the safety justification is self explanatory (Figure 7-13)):

1. Management of restrictions is adequate;
2. Applicable hazards are managed to closure or are conditionally closed and managed through restrictions. The Safety risk is ALARP;
3. Incident management is appropriate;
4. Train-signalling system is acceptably safe subject to adequate management of residual risk through restrictions.

Conclusion of the Safety justification was that a set of restrictions, dependencies and other safety measures has been identified which enabled the train operations associated with V2.01 testing to be performed at a level of risk which is tolerable and ALARP. Safety justification can be seen a subset of the reasoning model that is the System Safety Case for VLUP.

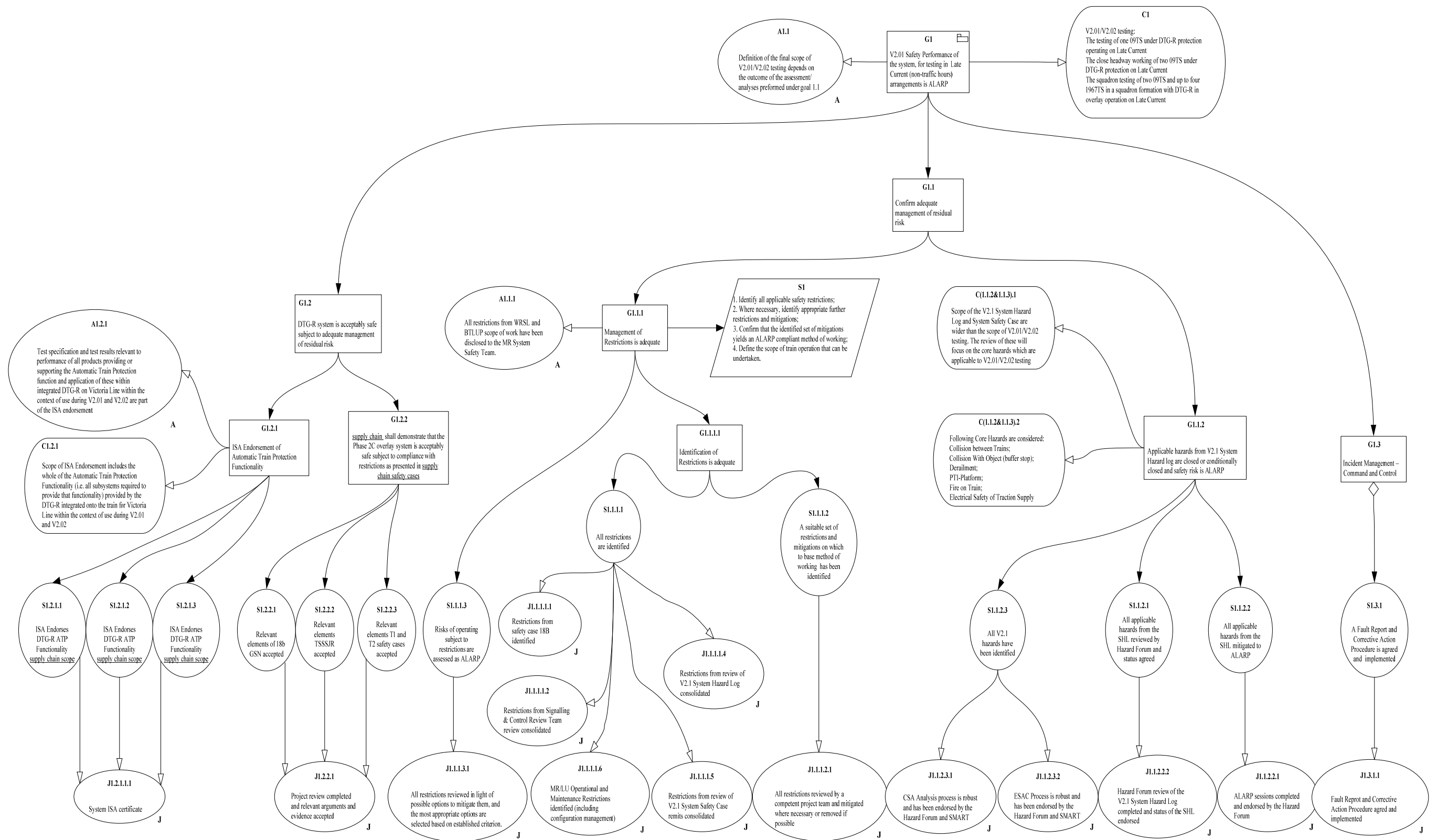


Figure 7-13: Example of Safety Justification produced in support of the VLUP Testing of the new Train and Signalling system (DTG-R signalling system in overlay)

7.8.2 Safety Case

In general, the safety argument about any undertaking should be based around the following lines of reasoning, for each of the 4 elements (as discussed earlier):

1. Objectives/Requirements:
 - a. Hazards, emerging from the change of the system, identified, analysed and managed;
 - b. Suitable safety targets identified, selected and achieved;
 - c. Safety performance of the system is commensurate with the ALARP principle;
- 2 Arguments including:
 - a. Completeness of the analysis and implementation of protection and prevention measures (mitigations, barriers and containment measures), requirements and targets;
 - b. Control of hazards on an individual basis including Qualitative Safety Arguments and/or Quantitative Safety Arguments;
 - c. Options and Impact analysis (is there anything else, practicable, that can be done to reduce the risk level further) including the practicability argument (qualitative or quantitative cost-benefit analysis), assessment and comparison of the costs of any proposed changes to the system against the reduction in risk levels with the acceptance/rejection criteria for selection of options;
 - d. Rationale for adequacy of safety management activities and implemented mitigations, requirements and safety targets;
 - e. Rationale for adequacy of evidence provided in support of the arguments;
3. Evidence of:
 - a. Comprehensive change safety management process followed;
 - b. Comprehensive processes used to identify, manage and close hazards including: HAZOP, HAZID, Functional Failure Analysis, FTA, Interface Analysis, Single Point Failure Analysis and Diversity Analysis with traceable detailed records of these activities;
 - c. The system design approach, including design of system architecture, use of a suitable means of checking for errors, including design reviews and the ability of the system to self-check;
 - d. Applicable standards and practices being identified (such as EN50126, EN50128, EN50129), followed and complied with;

- e. Use of a Problem/Fault/Data Reporting And Corrective Action System;
 - f. Work performed by the ISA (or Competent Independent Person) during the project;
 - g. Evidence of implemented protection and prevention measures (mitigations, barriers and containment measures), requirements and targets being achieved, including testing and verification and validation results;
 - h. Where novel process elements are employed, (e.g. by the introduction of new techniques not included in EN50126/8/9), a more extensive justification that they are consistent with the achievement of ALARP is required;
4. Context:
- a. Outline of the system to be changed;
 - b. Outline of the changes to be introduced to the system with their impact on the system performance;
 - c. Outline of the operational environment of the system, including the outline of the technical “operational envelope” of the system operating within the given environment under given operating conditions.

The System Safety Case Structure

On both, VLUP and SSL, the same philosophy to construction of the safety case has been adopted, in outline the safety argument is broken down into:

1. Introduction: Safety objectives, targets and requirements are outlined in this section (summary of point “1” above);
2. System Definition: This section provides context for the safety case (point “4” above);
3. Quality and Safety Management Reports: This section presents the Quality and Safety Management System adhered to during the life cycle phases of the system development/change (point “3” from “a” to “f” above);
4. Technical Safety Reports: This section of the safety case contains all safety reports related to the system. This section corresponds to main safety case parts, Objectives or Requirements, Evidence and Arguments. The context of this section is not a simple repetition of the previous two sections but goes into much more detail;
5. Related Safety Documents: This section provides references to all other related safety documents and documented processes used in support of the development

of the safety case.

For clarity of presentation and ease of appraisal, the SSC is structured as follows:

VOLUME 1: Presents a statement of safety objectives, confirmation if these have been achieved, and high-level summary of safety arguments and any outstanding safety issues for the railway system configuration stage. It contains the principal record of the safety arguments for the changes being implemented, and where they have a safety implication on the Project.

The Vol.1 is subject to endorsement, providing a key document input, by the acceptance bodies.

VOLUME 2: Contains safety arguments. It is structured around the core hazards and related safety goals and contains all the key Technical Safety Reports (TSR).

VOLUME 3: Contains the ‘evidence of safety’ in terms of compliance statements, including references to the key Verification and Validation (V&V) records, traceable audit information and close-out reports, Test Results, etc which support the Vol.1 and Vol.2 entries. This volume also refers to all other safety related documents, supply chain safety cases, Audit Reports, Test Logs, etc.

The sections for **Vol. 1 of the SSC** are as follows:

1. List of References
 2. Executive Summary - This section provides a high level SSC status overview:
 - a. Purpose and scope of submission for V2.1;
 - b. Status of the SSC and related activities including the status of previous submission;
 - c. Outline claim of the submission;
 - d. Status of identified programme risks related to the SSC delivery;
 - e. List of sections altered from previous submission;
 3. Introduction - This section consists of following subsections:
 - a. Objectives of the System Safety Case;
 - b. Aims of this volume;
 - c. Scope of the System Safety Case;
 - d. Definitions;
 - e. Abbreviations;
 4. Proposed Submissions - This section presents the proposed submissions of the SSC.
 5. System Definition:
 - a. Overview of VLU;
-

- b. System Outline;
- 6. Structure and Status of the System Safety Case - This section consists of the following subsections:
 - a. Position of this Document;
 - b. Format of the SSC;
 - c. Status of the SSC;
 - d. Changes from previous submission;
 - e. Comparison with EN50129;
- 7. Methodology - A summary of the methodology followed during development of the SSC is outlined in this section, as follows:
 - a. Safety Goals;
 - b. Method of Safety Analysis;
 - c. Structure of Safety Argument;
 - d. Change Safety Analysis process;
 - e. Role of ISA;
- 8. Safety Justification - This section provides an overview and summarises the status of the safety arguments for the V2.1 project stage, to be detailed in Volume 2.
 - a. Completeness of the coverage of the risk;
 - b. Train accidents;
 - c. Movement accidents;
 - d. Non-movement accidents;
 - e. Complete set of sub goals;
 - f. Safety Arguments Status Report;
 - g. Outstanding Safety Issues – Summary;
 - h. Conclusions;
 - i. Overall GSN;
- 9. Next submission - The scope and objective of the next SSC submission is outlined in this section;
- 10. Implementation –Delivery:
 - a. Responsibilities;
 - b. Liaison with LU;
 - c. Liaison with Supply chain;
- 11. Appendix I: ADCs;

The following sections comprise **Vol. 2 of the SSC**:

- 1. Overview:
 - a. Scope;
 - b. Aim;
 - c. Outline of overall safety argument;
 - d. Structure of SSC Vol 2.;
- 2. System Definition:

- a. System description;
 - b. Operational envelope of the system;
- 3. Quality Management report:
 - a. Roles and Responsibilities;
 - b. Lifecycle Issues;
 - c. Standards;
 - d. Audits and Assessments;
 - e. Supplier management;
 - f. Controls;
 - g. Configuration Management;
 - h. Project Quality Management Training;
 - i. Outstanding Issues;
- 4. Safety Management Report:
 - a. Roles and responsibilities;
 - b. Safety lifecycle;
 - c. Safety analysis;
 - d. Safety Standards;
 - e. Safety audit and assessment;
 - f. Supplier management;
 - g. Safety controls;
 - h. Configuration management;
 - i. Project safety training;
 - j. Outstanding issues;
- 5. Core Hazard/Safety Goal:(NOTE: This section is repeated for each Safety Goal):
 - a. Scope;
 - b. Description and Process model;
 - c. Change Safety Analysis;
 - d. Derivation of Safety Acceptance Criteria;
 - e. Safety arguments;
 - f. Outstanding Safety Issues;
 - g. Related Safety Documentation;
 - h. Conclusion;
- 6. Appendix I: Assumptions, Dependences, Caveats;
- 7. Appendix II: Migration Plan;
- 8. Appendix III: Project Assurance Plan.

The following sections comprise **Vol. 3 of the SSC**:

- 1. Overview;
- 2. Subsystems: summary of safety documentation/evidence and its status.

The safety case structure recommended in EN50129 is widely recognised as representing good practice in the production of safety cases and is used well beyond

the Standard’s nominal scope of electronic systems for railway signalling. Figure 7-14 shows how the structure adopted for the SCC encompasses all the material required by EN50129 and builds into an equivalent structure.

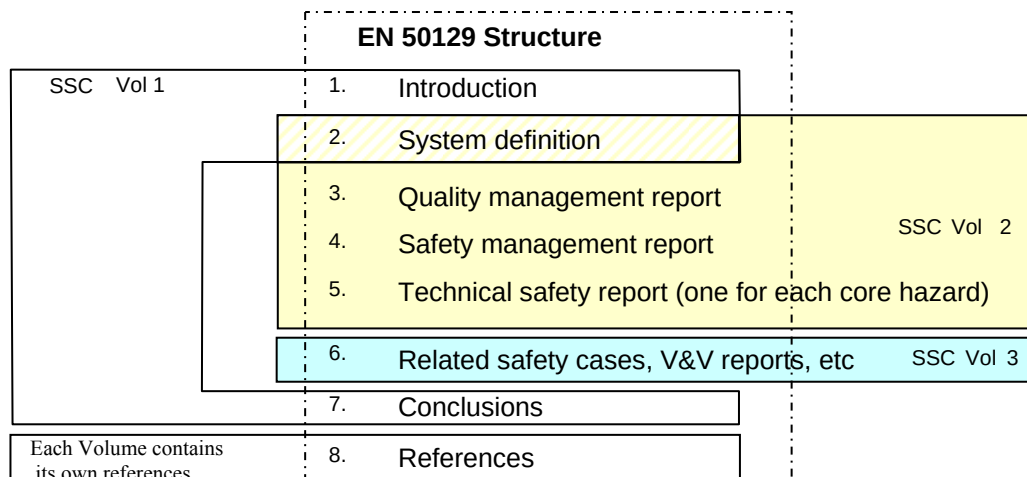


Figure 7-14: SCC mapped onto EN50129

This structure is compatible with the safety case format recommended by CENELEC EN50129 standard, but supports the focus on the control and management of the hazards and consequences.

Victoria Line Upgrade Programme – System Safety Case

the author structured the System Safety Case (SSC) as outlined above. Heart of the SSC is the Volume 2 and outline of the VLUP System Safety Case is presented on Figure 7-15 below.

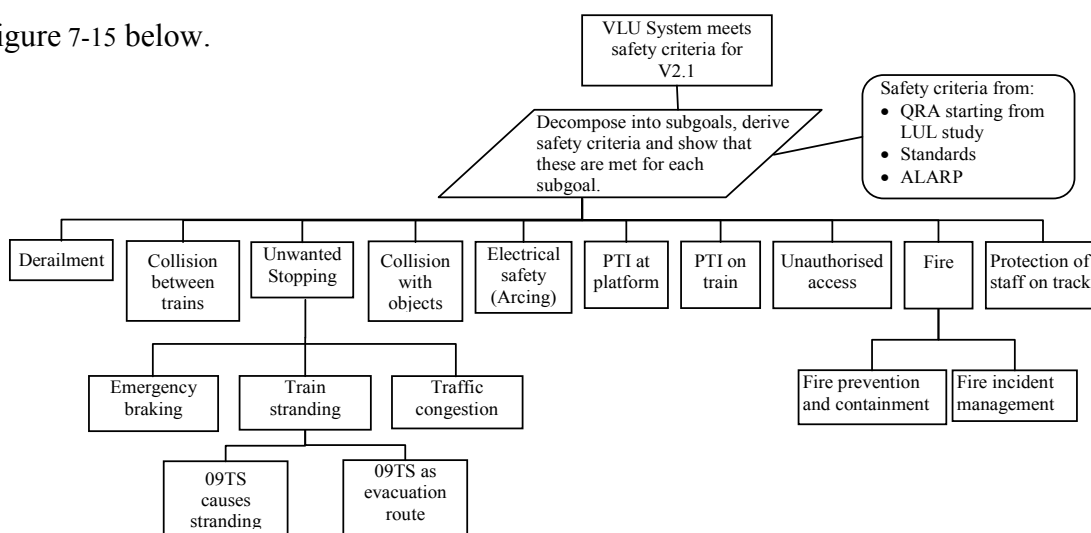


Figure 7-15: VLUP GSN- Top level

As the management organisation of the VLUP is relatively simple, there was no need for GSN presentation of the sections dealing with Quality management and Safety management. The GSN has been developed for each safety goal/core hazard. As an example, Figure 7-16 , we will discuss a GSN for “Collision between trains” core hazard, with related top safety goal being “Risk of collision between trains meets criteria”.

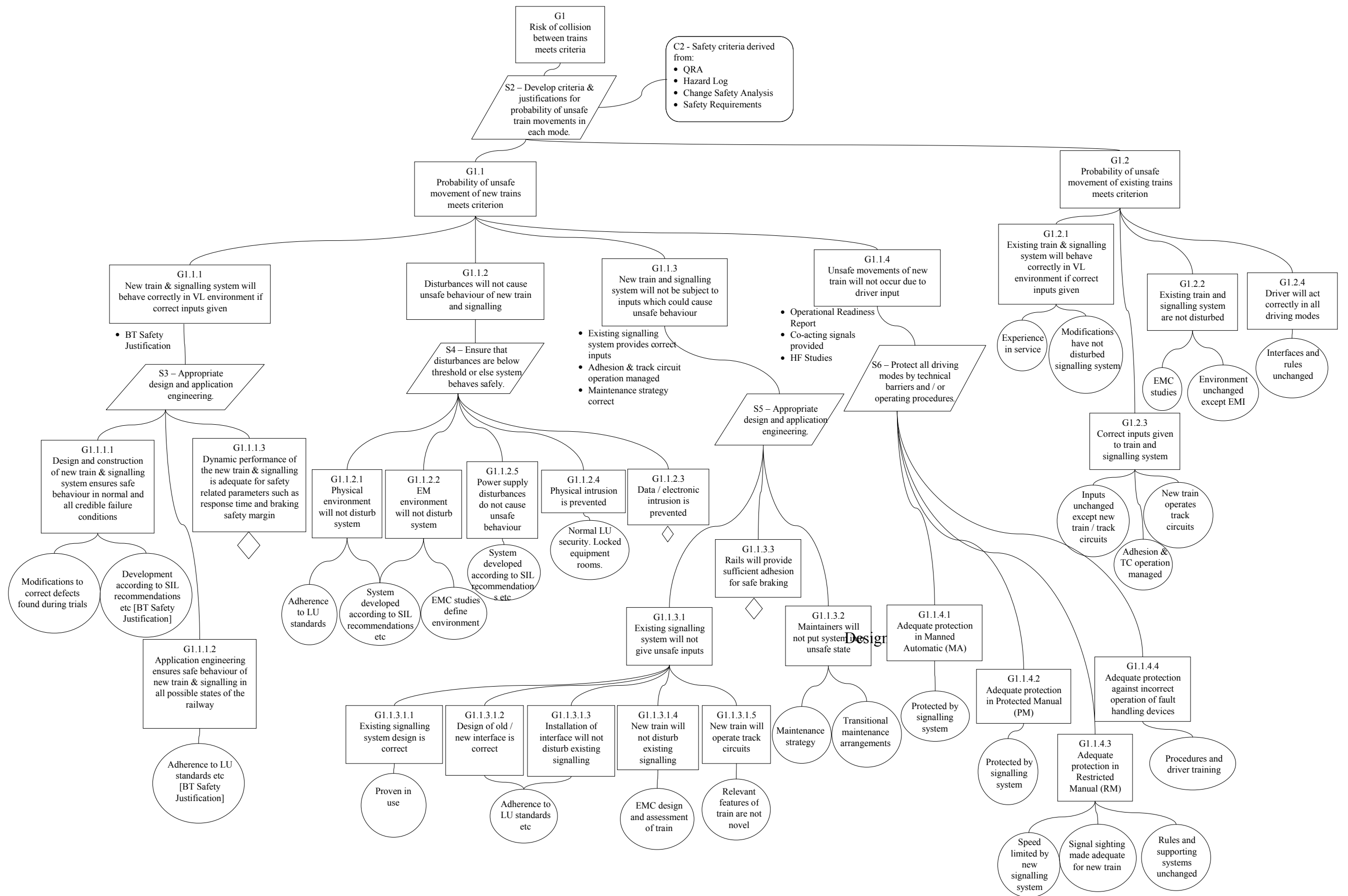


Figure 7-16: Collision between trains GSN (VLUP System Safety Case)

The process model is used to set a context for the safety case argument and to focus specific justification for each of the main areas of concern, indicated by the GSN. For the relevant phase of the project, testing of the new trains in traffic hours, the only elements of the overall process for train movements represented by the process model Figure 7-5 which are changed from the existing Victoria Line are those associated with the introduction of the new train and signalling system. The changes comprise:

1. Introduction of new train and signalling system;
2. Modification to existing signalling system to provide interface to new system;
3. Provision of co-acting lineside signals where needed for sighting from new train;
4. Changes to driver's task associated with design of new train and signalling;
5. Changes to activities of signalling, track and rolling stock maintainers.

The outline of the safety argument is as follows:

1. The new train and signalling system will behave correctly providing they are not disturbed and providing they do not receive inputs which could cause unsafe behaviour;
2. The potential disturbing factors in the environment of the Victoria Line will not cause unsafe behaviour of the new train and signalling system;
3. The probability of inputs or actions which would cause unsafe behaviour being applied to the new train or signalling system is consistent with the safety acceptance criteria;
4. The introduction of the new train and signalling system will not adversely affect the behaviour of the existing trains with regard to the risk of collision.

In addition, special consideration is given to two particular operational activities; moves towards buffer stops and rescue of failed trains. The risk of train collision is made equal to or lower than the value derived from the LU QRA model by the combination of technology developed to appropriate levels of safety integrity, established good practice in engineering, and the application of effective safety management to operations.

Detailed arguments for each of the goals relating the safety justifications with evidence and providing the logical framework has been developed for each of the safety goals from the GSN. The conclusion of the System Safety Case was that the safety risk is not materially impacted by the operation of the pre-series trains in passenger Traffic Hours and residual safety risk has been reduced as low as reasonably practicable. This was subject to:

1. The imposition of a number of identified restrictions and

2. Confirmation of the conclusions in the system safety case to be gained upon acceptance of the supply chain safety cases by the programme.

Subsurface Lines Upgrade Programme – Hierarchy of Safety Cases

As already outline the Subsurface Lines Upgrade Programme (SUP) delivery organisation is a hierarchically structured with many (40 projects) delivering at different timescales to a common objective at a number of migration stages. This arrangement dictates a structure and management of a delivery of the safety cases in support of the projects and the overall programme as illustrated by Figure 7-2, Figure 7-3, and Figure 7-4 earlier. A model of the hierarchy of safety cases, which the author established, is illustrated by Figure 7-17 below.

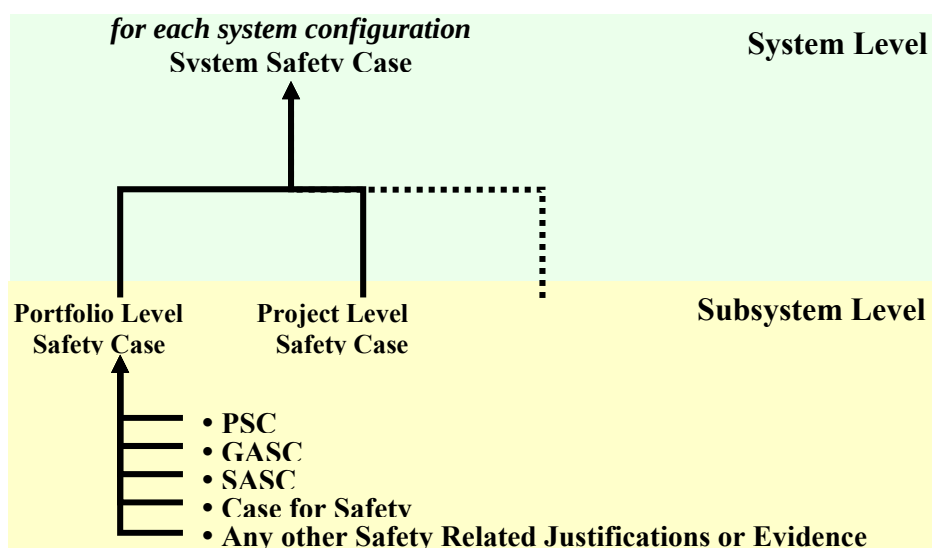


Figure 7-17: Hierarchy of safety cases and justifications/evidences

The subsystem level safety cases are delivered and submitted for approval as and when required prior to individual projects' works being delivered and most often in advance of the system safety case delivery (some of the project level deliverables are completed at the same time as the system commissioning and are therefore delivered and submitted at the same time with the system safety case but to different approvals/acceptance bodies). However, in order to secure delivery of the complete safety argument, the system safety case structure and fact net must be completed well in advance, with all the subsystem level safety arguments relevant to the system level argument identified and "completed" as part of the subsystem level safety cases delivery and acceptance. This is illustrated by Figure 7-18 and Figure 7-19 below. The system level safety argument for Train Movement Accidents, outlined by the GSN (Figure 7-18), covers the complete system. Each of the goals in this particular example are influenced by system changes being delivered by more than one project, as illustrated by Table 20 below.

Goal	Goal Description	P r o j e c t s	Signalling Immunisation	Legacy Signalling	Signalling Contactor	Train Arrestor Project	Maximum Safe Speed	Rolling Stock	NDUP Project	Structural Analysis Project	ICSS Project	OPO TT CCTV Project	ELLCCR	Stopping Mark Project	DC Traction Power Upgrade	Platform Lengthening	Track Assessment	Operations	System
M1 G902	The risk that the Earthing & Bonding arrangements are incompatible with the existing railway is reduced in line with risk principle		•	•	•	•		•	•		•	•			•	•			
M1 G903	The risk of the movement authority not being visible to the train operator in all rolling stock is reduced in line with risk principle			•		•		•	•										
M1 G904	The risk that the increased length of S Stock is not compatible with signalling layout and clearances is reduced in line with risk principle			•		•		•	•										
M1 G910	The risk that any train is not detected by the Signalling System is reduced in line with risk principle		•					•											
M1 G916	The risk that the driver/staff can introduce an unsafe state in the system is reduced in line with risk principle		•	•				•	•										
M1 G918	The risk an unsafe state is introduced in maintainer equipment is reduced in line with risk principle		•	•				•	•		•	•							
M1 G922	The risk that any objects (e.g. trackside, platform mounted or the platform, structures etc) infringes the Kinematic envelope of the rolling stock is reduced in line with risk principle		•	•		•	•	•	•		•	•			•				
M1 G957	The risk that any products/ subsystems/systems cannot be supported over the complete lifecycle is reduced in line with risk principle		•		•						•		•		•				
M1 G958	The risk that any products/ subsystems/systems cannot be maintained over the complete lifecycle is reduced in line with risk principle - (includes equipment to be located in a position where it can be maintained in safety is reduced in line with risk principle)		•	•	•	•		•	•		•	•	•		•				
M1 G959	The risk that any products/ subsystems/systems is not sufficiently reliable so as to effect the safety performance over the complete lifecycle is reduced in line with risk principle		•	•	•			•	•		•				•				

Table 7-20: Apportionment of responsibility for engineering safety management activities and delivery of evidence across the programme work packages

The GSN elements coloured blue are the goals related to the scope of change delivered by the Immunisation portfolio projects.

Following from that the Immunisation portfolio GSN and the safety case were produced, demonstrating the justification for safety and providing the evidence in support of the safety argument. This is illustrated by Figure 7-19 below.

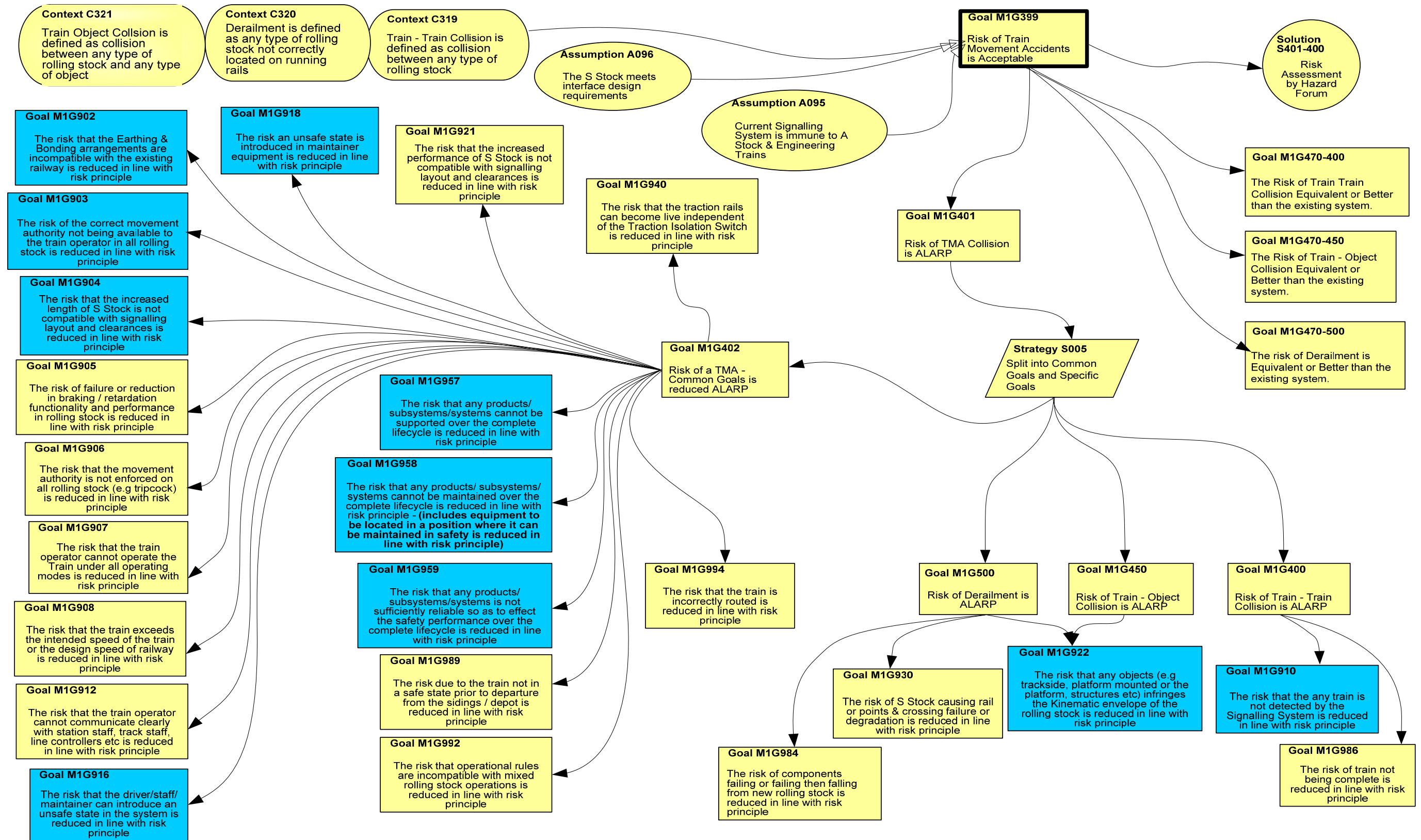


Figure 7-18: SSL system level train movements accidents GSN

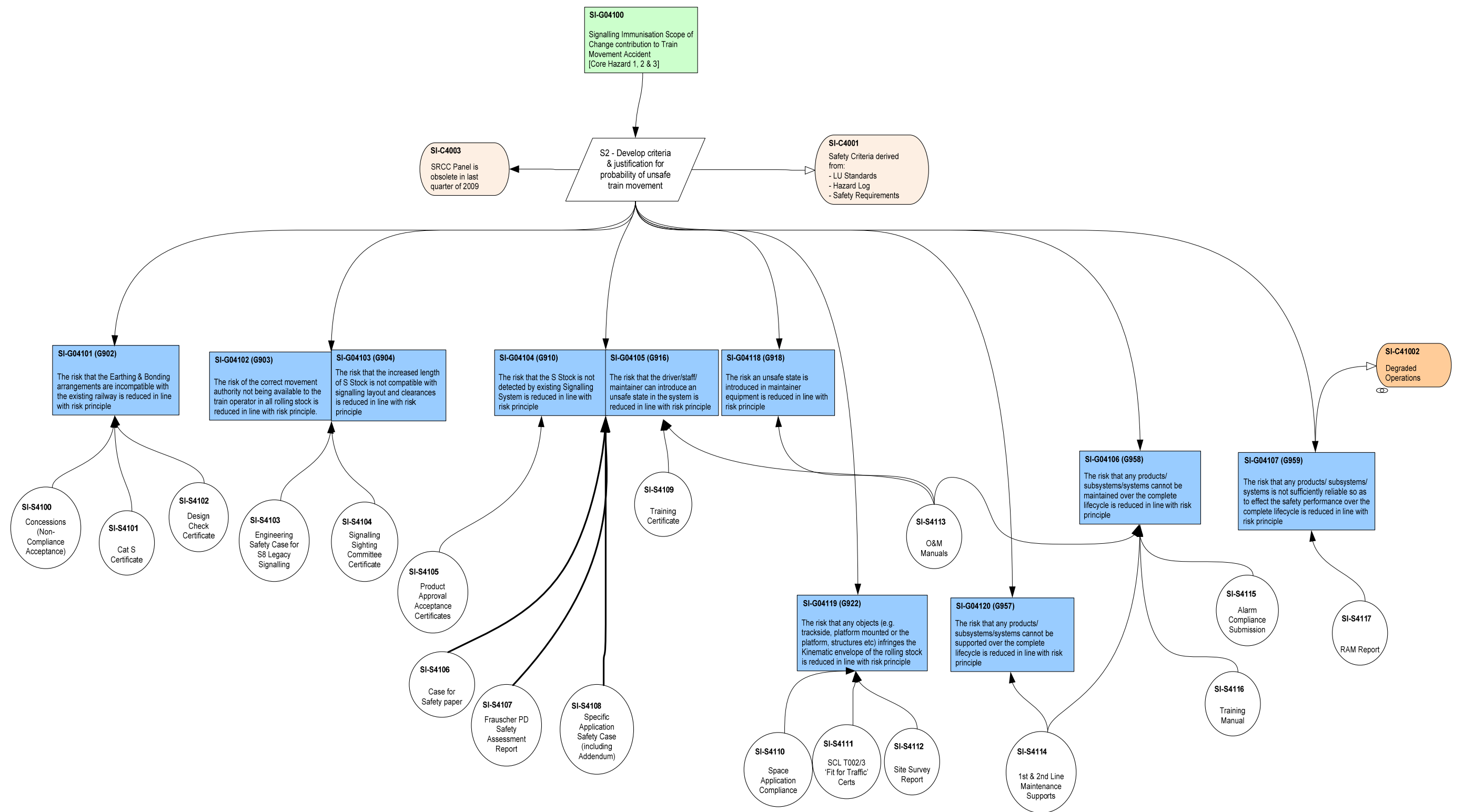


Figure 7-19: SSL project portfolio (subsystem) level train movements accidents GSN

The goals (coloured blue) correspond directly to the system level goals and represent the contribution to the risk from the immunisation portfolio implemented changes to the system safety performance in these particular areas. For each of the goals, a remit has been produced, agreed with and passed to the actionee.

This process supports assurance of completeness of the safety argument and justification.

In support of the clarity of delivery and structure of documentation, the author produced the hierarchical document tree, an example of which for system level and the immunisation portfolio level is shown by Figure 7-20 below. All of the arguments and evidence at project level is summarised at the project safety cases as presented in listed documentation.

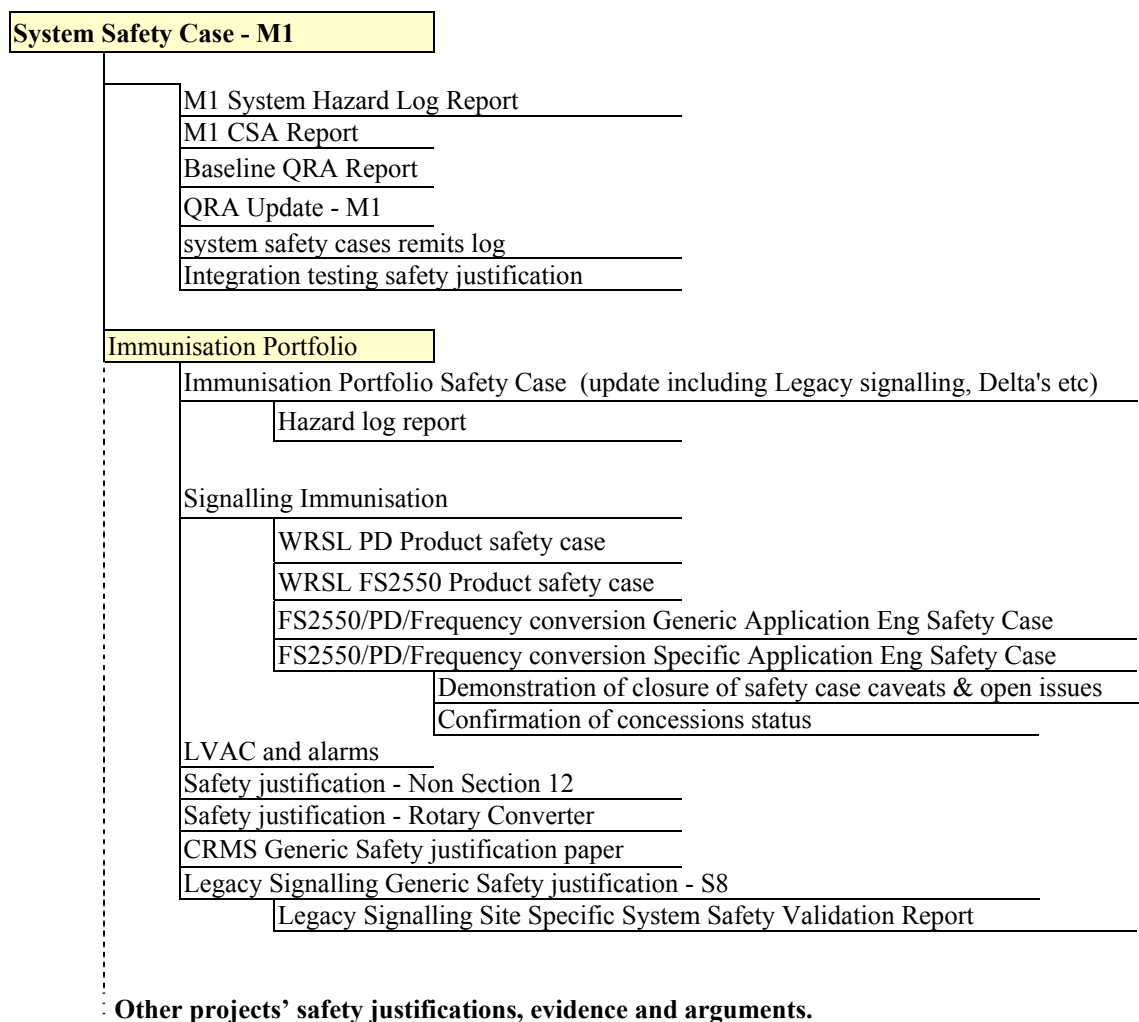


Figure 7-20: SSL System safety argument document tree

7.9 Assertion of completeness of analysis and assessment of uncertainties

An approach to assurance of completeness of the system understanding and completeness and correctness of change safety analysis has been discussed earlier and

the same processes and methodologies were (and still are) successfully applied on both VLUP and SSL. This will not be further discussed here.

However, during the work on VLUP and SSL an additional type of completeness argument has been identified as required.

7.9.1 Completeness of the safety arguments/facts net

As already mentioned earlier, the completeness of the safety arguments net, can be classified in three kinds:

1. Wholeness of lines of reasoning explored;
2. Sufficiency and Completeness of evidence provided in support of these arguments;
3. Certainty of evidence provided in support of these arguments.

Wholeness of the logical fact net, that is the safety case, is being assured by adherence to the Change Safety Analysis, Risk Assessment and Management process for its development. In addition the fact net must be transparent throughout its own life cycle, involving all the necessary competences in its development and review.

Use of GSN or some other form of graphical presentation of the fact net, certainly supports the verification of wholeness of the safety arguments. Substantiation of Sufficiency and Completeness of evidence differs depending on the subject, varying from a simple well understood problems, for which the evidence can be a simple check or a 100% test of all functionalities provided by the relate subsystem, to complex distributed, software based safety critical control systems, where a 100% test is practically impossible and the evidence is likely to consist of some practical testing (with justification of the tested sample being based on statistical analysis) and the evidence of adherence to adequate processes including use of advance development and analysis tools. Whichever type of evidence is being provided, the justification for sufficiency must be made.

Certainty of evidence depends on the type of provided evidence. In case of a proof based on a physical measurement (in a very general sense), the certainty is relatively easy to prove through use of well known methods for determination of precision of measurement. However, in case of non-measurable, intuitive, evidence, typically related to proof of adherence to processes and application of good practice and standards, it is much more difficult to determine the level of confidence in available information. The usual method to support this kind of evidence is by an audit and

monitoring of the initial failure rates through FRACAS/DRACAS system for more frequent than expected failures of the system as an indication of inadequate processes in place or existing mitigations although being implemented not being effective.

7.10 Management and Reporting (Presentation of results)

7.10.1 Management

Planning and management related to safety management activities is not different to management of any other engineering undertaking, apart from the following activities specific to engineering safety management (common planning and management will not be further discussed):

1. Management of the hazard logs;
2. Management of the operational restrictions;
3. Management of the safety case delivery.

These are related and to great extent overlapping.

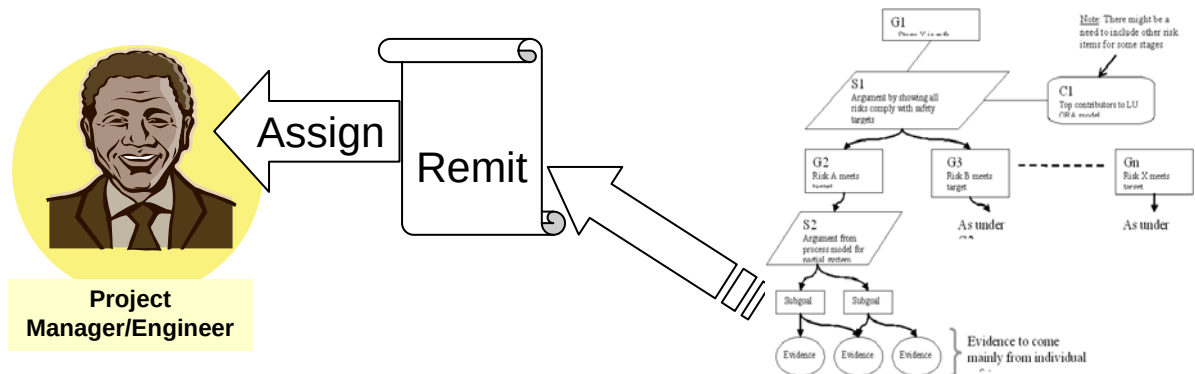
Hazard log, as already mentioned, holds a record of all the hazards and related change safety activities. Apart from making sure that all the records are kept up to date and configuration controlled, which will be discussed later, the hazard log is a tool for control and management of hazard log actions. Each action needs to be allocated to owner with a clear and concise description of the action and what action is expected to deliver.

Operational restrictions need to be managed and controlled with the same rigour as the hazard log. During identification and analysis of the restrictions it is necessary to identify the evidence required and the “authority” to remove or relax the restriction. No restriction should be removed without the documented agreement from the identified authority.

Most often delivery of the safety case is dependent on input from people or teams other than the safety case author or the engineering safety team. On SSL and VLUP programmes, delivery of the safety cases has been managed through the remits. At project level, Project Managers are responsible for delivery of all documentation on projects including that required to support delivery of the system safety case.

It is the Project Manager and delegated Project Engineer responsibility to ensure that evidence is collated and controlled that will support all of the arguments for safety case, including the maintenance and operations readiness and RAM performance acceptability.

The system safety team identifies the safety arguments and evidence requirements and develops remits for delivery in support of the system safety case by the Project Manager or Engineer.



- Structure arguments & justifications supporting the safety case using Goal Structured Notation;
- For each argument/justification produce a remit;
- Assign it to a project manager/project engineer to deliver.

Figure 7-21: Delivery management of the Safety Case

Management of safety case via remits, allows for reporting against the remits delivery as KPIs and monitoring of the progress.

In order to de-risk the assurance regime, for each system configuration several versions of the system safety case were submitted for review well in advance of the commissioning (this strategy is still being followed on both projects). As represented by the Figure 7-22, below, following approach was successfully implemented:

1. As early as possible a template document, indicating structure and main areas of discussion is submitted for agreement and approval;
2. A first draft with 85% to 95% of requirements identified and all evidence items intended to support these identified and related arguments completed subjected to review and approval by all stakeholders prior to final commission enabling submission;
3. A system safety case with all requirements identified, all evidence items intended to support these identified and most available, related arguments completed submitted for approval to allow commissioning to happen;
4. Due to complexity of the changes introduced to the system, a post commissioning system safety case update is submitted in order to close out any outstanding issues and enable the review of the adequacy of implemented mitigations and temporary mitigations.

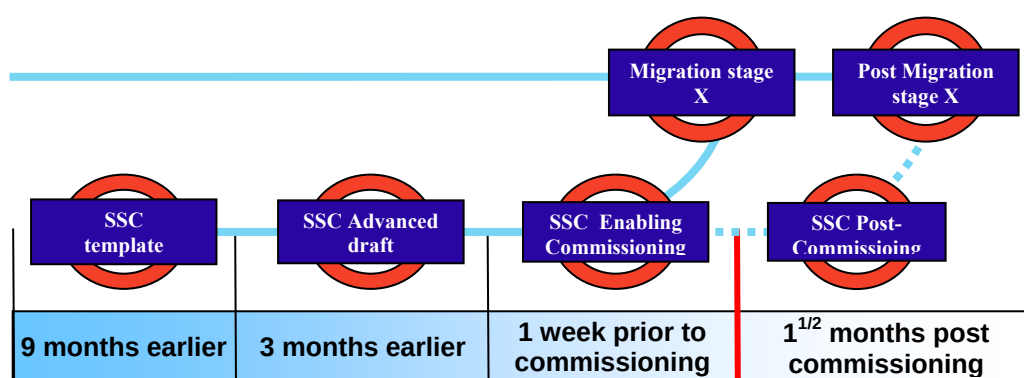


Figure 7-22: Typical programme of submissions.

7.10.2 Reporting

The author identified five types of reporting during implementation of the framework:

1. Analysis reporting. These reports present the analyses carried out and are usually submitted for approval and acceptance in preparation for commissioning of the system change. These reports should have the same general structure as the safety case; objective or requirements, arguments, evidence and context;
2. Analysis records, are used to create and auditable trial of evidence gathering in support of the analysis reports. These are used as evidence, referred to from the safety case;
3. Management-planning. Necessary safety management activities should be identified early in the project, planned and agreed within the project as well as with the regulatory and acceptance bodies. The plans need to be recorded and regularly updated to support auditable trial and continuity throughout the life of the project;
4. Management-implementation. Implementation of actions resulting from the change safety analysis and management activities, should be controlled through remits agreed between the actionee and the safety team;
5. Management-progress monitoring. On any project it is necessary to monitor progress of delivery. With regards to change safety management process, progress monitoring should be done through monitoring of the remits.

List of reports that have been identified and are being produced is presented in Table 7-21 below.

Directly related reports are indicated by outline numbering.

Report	Report category
1. Safety Case:	Analysis reporting
1.1 Safety Cases Remits;	Management-implementation
1.2 Remits Progress Reports;	Management-progress monitoring
2. Other safety cases, justifications & documents;	Analysis reporting
3. Hazard Log Report:	Analysis reporting
3.1 Action Remits;	Management- implementation
3.2 Hazard Forum Minutes;	Analysis record
3.3 Safety Requirements Forum Minutes;	Analysis record
3.4 Actions progress report;	Management-progress monitoring
4. Restrictions Register;	Management- implementation
5. Hazard report;	Management-progress reporting
6. CSA Report;	Analysis reporting
6.1 CSA Briefing;	Analysis record
6.2 ICSA Records;	Management- implementation
6.2.1 Change Requests;	Analysis record
6.2.2 ICSA Briefing;	Analysis record
7. QRA Report:	Analysis reporting
7.1 QRA Models;	Analysis record
7.2 QRA Data log;	Analysis record
7.3 QRA Change Register;	Analysis record
8. Process Models Report;	Analysis reporting
9. QRA Development Plan;	Management-planning
10. Safety Audit Plan;	Management-planning
11. Acceptance and Certification Strategy;	Management-planning
12. Engineering Safety Management Plan.	Management-planning

Table 7-21: Reporting - Change Safety Management process

7.11 Configuration Control, Continual Appraisal and Knowledge

Management

Within the change safety management process a number of different configurable data items exist:

1. System change data:
 - a. System Change scope and scope changes;
 - b. System configuration data;
 - c. Assumptions and Dependences;
2. Safety analysis data:
 - a. Hazard log data;
 - b. Risk assessment information (qualitative and quantitative);
 - c. QRA data;
 - d. Incidents and Accidents data;
 - e. Safety related documentation;
 - f. Operational Restrictions/Caveats;
3. Safety performance monitoring data:
 - a. FRACAS/DRACAS systems;

- b. Incidents reporting system;
- 4. Management data:
 - a. Planning;
 - b. Implementation and progress monitoring.

Relationships between these are described in Figure 7-23 below.

System change data enables and provides input into the system analysis. All of these must be strictly configuration controlled, because the change to the system data may have impact on the system safety performance. Frequent appraisal of how correct and current these information is, is crucial. Safety analysis and safety performance monitoring data are critical to development of a suitable, applicable and convincing safety case. These must be configuration controlled as well, but in addition to that, these data should be subjected to continual appraisal, throughout the life of the project, and once the project is completed, it shall be handed over to the infrastructure owner, it needs to be appraised until the system is decommissioned or upgraded when the new cycle of the safety management will began. The management data is used to record the processes and monitor the progress towards a successful delivery for the safety argument. Therefore this data does not have to be strictly configuration controlled but needs to be sufficiently current to enable appropriate progress monitoring.

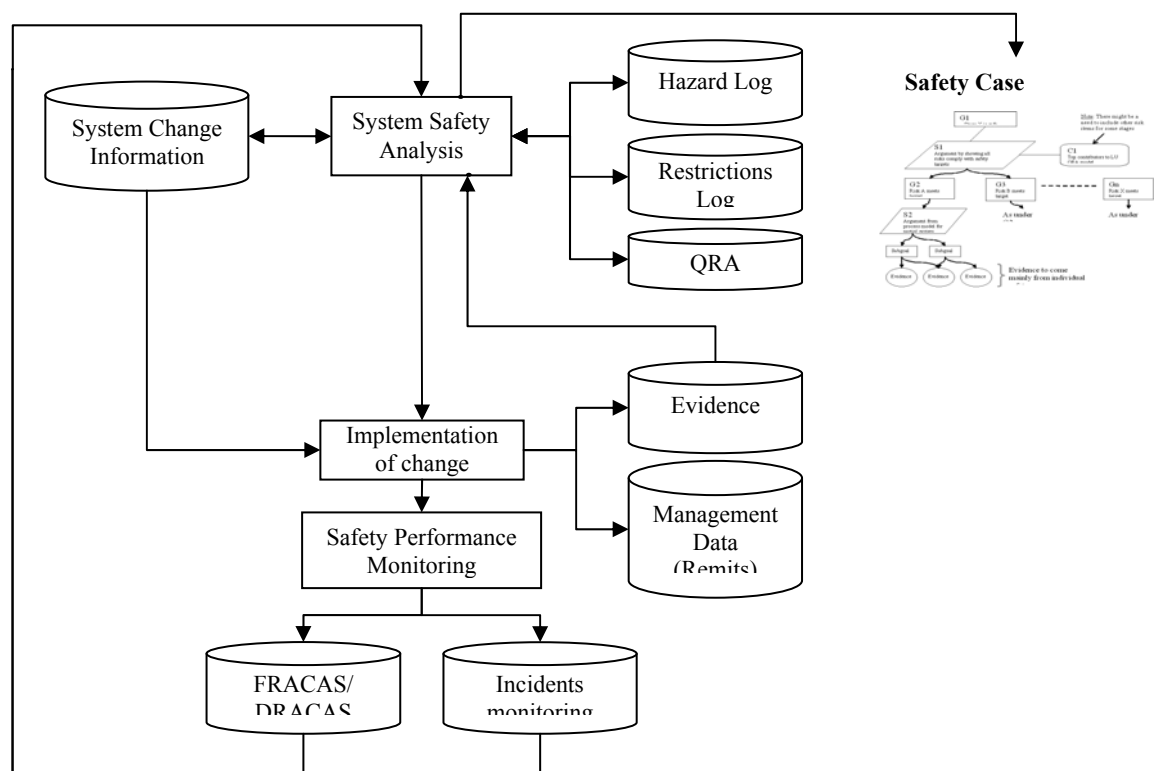


Figure 7-23: Configurable data items

In line with the recommendation from the Yellow book (RSSB, 2007) some of this information is contained within the hazard log (as described earlier) and configuration

control of it is managed through the parts of the hazard log itself.

Journal The Journal describes all amendments to the Hazard Log, in order to provide a historical record of its compilation and provide traceability. For each amendment it contains:

- 1 The date of the amendment (not necessary if a diary format is used);
- 2 A unique entry number;
- 3 The person making the amendment;
- 4 A description of the amendment and the rationale for it;
- 5 The sections in the Hazard Log that were changed.

Directory of safety related documents. The Directory, provides an up-to-date reference to every safety document produced and used by the Project. The documents referred to include the following, where they exist:

1. Safety Plan;
2. Safety Requirements Specification;
3. Safety standards;
4. Safety Documents;
5. Incident/accident reports;
6. Analyses, assessment and audit reports;
7. Safety Case; and
8. Correspondence with the relevant Safety Approvers.

For each document the Directory includes the following:

1. A unique reference;
2. The document title;
3. The current version number and issue date; and
4. The physical location of the master.

Hazard Data (including safety requirements). Every identified hazard is recorded. For each hazard, the information listed below is recorded as soon as it becomes available and strictly configuration controlled. Data collected during Hazard Analysis and Risk Assessment is contained within the Hazard Log:

1. A unique reference;
2. A brief description of the hazard including the system functions or constituents affected and their states that represent the hazard;
3. The causes identified for the hazard;
4. A reference to the full description and analysis of the hazard;

5. Assumptions on which the analysis is based and limitations of the analysis;
6. The severity for the related accident, the likelihood of the hazard occurring and the likelihood of an accident occurring with the hazard as a contributing factor;
7. The predicted risk associated with the hazard;
8. Target likelihood for its occurrence;
9. A reference to all Safety Requirements associated with this hazard or with related causes or protection measures;
10. A reference (and description) to the system interface or object:
 - a. Whose change is the source of cause or hazard;
 - b. To which a protection measure is related;
11. A reference (and description) to related QRA elements (base and top events, gates, etc);
12. The status of the hazard;
13. If the hazard is not closed or cancelled, then the name of a person who is responsible for progressing it towards closure;
14. A description of, or a reference to, the action to be taken to remove the hazard or reduce the risk from the system to an acceptable level. This includes:
 - a. A statement as to whether the hazard has been avoided or requires further action (with a justification if no further action is to be taken);
 - b. Details of the risk reduction action to be taken;
 - c. A discussion of the alternative means of risk reduction and justification for actions considered but not taken;
 - d. A comment on the need for accident sequence re-evaluation following risk reduction actions;
 - e. A reference to any design documentation that would change as a result of the action;

Incident Data. At the time of writing this thesis no incidents occurred. However, in future all incidents that have occurred during the life of the system or equipment are to be recorded here, identifying the sequence of events linking each accident and the hazards that caused it.

For each incident the following will be provided:

1. A unique reference;
2. A brief description of the incident;
3. A reference to a report describing an investigation of the incident; and
4. A description of any action taken to prevent recurrence, or justification of the decision not to take any.

Consequence/Accident Data. Every identified possible consequence is recorded, including the possible sequences of events linking identified consequence with the hazards that may cause it. For each consequence the following is provided:

1. A unique reference;
2. A brief description of the potential consequence;
3. A reference to a report giving a full description and analysis of the consequence sequence;
4. A risk assessment information (either comparable, using earlier outlined methodology or quantified data); and
5. A list of the hazards and associated consequence sequences that could cause the consequence.

Operational Restrictions are being managed by a centralised Restrictions register. As operational restrictions are in fact temporary mitigations these need to be treated with the same rigour as the hazard log. Table 7-22 is an example of the record.

Ref	Description	Group	Rationale	
R014(a)	The full performance key switch shall only be operated (to select full performance) whilst in an Engineer's Current Area. At all other times the key switch shall be OFF.	Rollin stock - power	Full execution of test	
Action	Actionee	Status	Criteria for Removal	Removal Authority
Ensure train is Inter-Running mode when outside Engineer's Current Area.	Lead Train Master.	Open	Confirmation of successful conclusion of all tests requiring operation at "Full Performance" and removal of key switch mode.	Head of Rolling Stock Engineering SUP (C Holmes), Transportation
Notes			Evidence or Action	
Revised 16th November 2009 following installation of Mod No. SSL1509.			#N/A	

Table 7-22: An example of the restriction's register record

QRA related information can be split into two categories; data and logic. Model data needs to be regularly reviewed and confirmed against the latest incident data. The logic of the QRA model, once the models has been completed (including review for correctness), needs to be reviewed after each change to the system. Usually tools used for QRA modelling have the data storage facilities. On both VLUP and SUP, Fault

Tree + software has been used for modelling. All of the modelling data is stored within the tool's data repository. The configuration control is implemented through the tool following a change control process.

FRACAS/DRACAS: failure/defect reporting and corrective action system is in place on both VLUP and SUP. This is a standard process and will not be further disused here, apart from mentioning that it is essential for the information from FRACAS/DRACAS system to be reviewed against the records in the hazard log and the restriction log to confirm that the mitigation in place are working and are sufficient and that there are no missing causes in the hazard log.

System Change Information: as the system is being changed it is necessary to keep the information about the change up to date and ensure that the system description is complete and correct. The process already earlier in this thesis, has been successfully implemented on both projects and is working.

Incidents monitoring is implemented across the LU. All the incident reports are subjected to analysis by the engineering safety team. Any relevant information is assessed and if appropriate used to update the QRA and/or hazard log.

Remits are used in support of management process to convey the detail of action that needs to be taken to the actionee including the timescales for delivery. As already explained, the status of remits is used as indication of progress of the safety case delivery. An example of a remit is presented below in Table 7-23.

Task Id.		Context		Task Description
BTLUP1		There are numerous items in the BTLUP Hazard Log relevant to train signalling system, all of which are controlled or mitigated by the measures on which the safety arguments are based.		Provide regular update on the status of the BTLUP Hazard log including: • clear and unambiguous statement of arguments in support of closure of hazards; • an assessment of residual risk (ALARP argument); • reference to relate the hazard log entry to the process model interface.
SSC Section				
Collision and Derailment				
SSC reference				
Add New section on Project hazard logs				
Delivery	Milestone	Owner	Status	Type of response agreed
dd/mm/yy	Delivery of the hazard log report for V2.1 system configuration with all relevant hazards closed	Name	Draft response received	LUP: Delivery of an update to the hazard log report with all hazards closed or conditionally closed. LUP: Confirmation that all hazards have been transferred from MR to BT. The WRS hazard log report will be available by the end of May.

Table 7-23: An example of the remit

7.11 Chapter Conclusions

In this chapter the author outlined and analysed the results of a real life application of the proposed framework. As part of this work the author identified some minor gaps in the framework, developed missing processes and methodologies. These have been tested and analysed as well. Detailed conclusions drawn from this are presented in the next chapter

CHAPTER 8: CONCLUSIONS, CONTRIBUTION AND SUGGESTIONS FOR FUTURE WORK

8.1 Conclusions and contribution

This section summarises the findings of the research and identifies my contribution to the knowledge and practice of System Safety. The structure of this section is outlined by figure below.

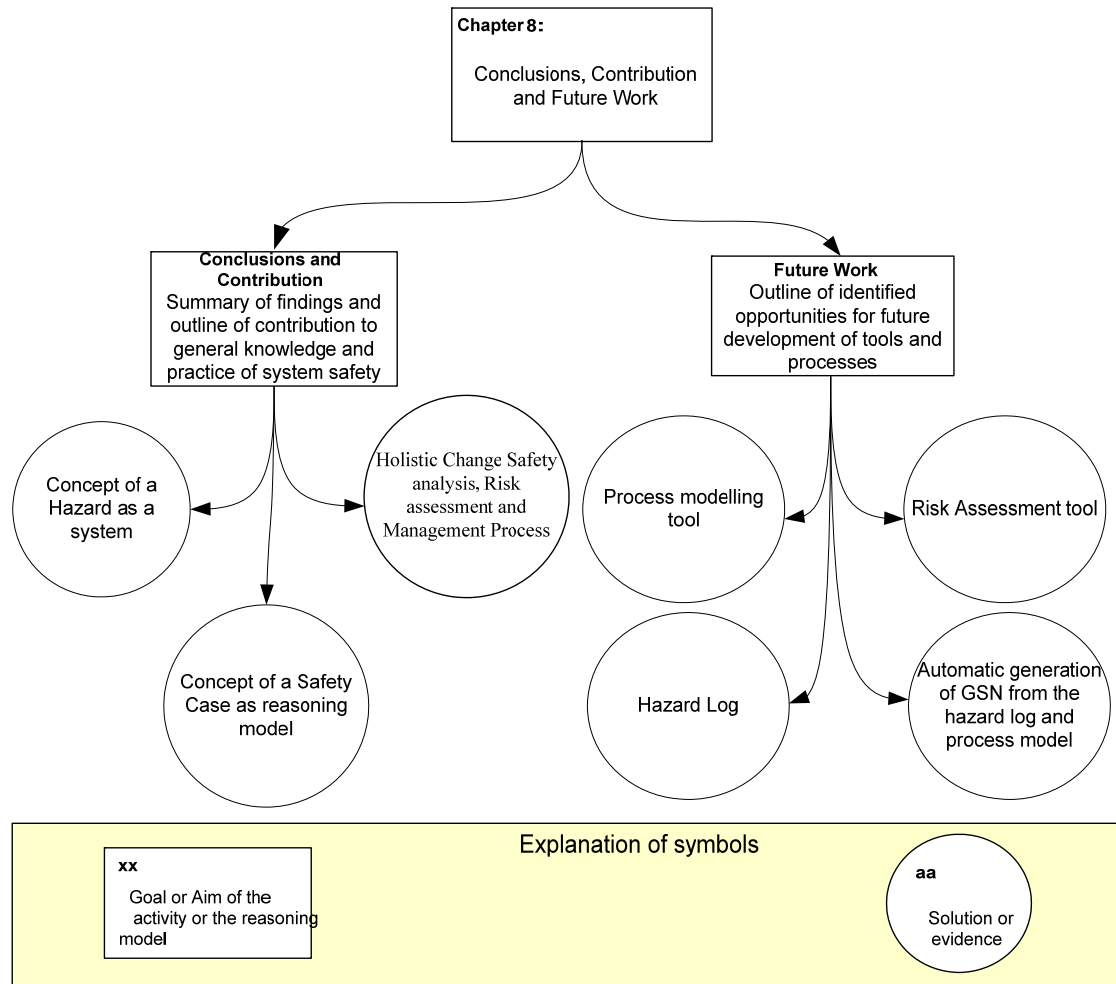


Figure 8-1: Structure of Chapter 8

8.1.1 Overall summary

the author completed a thorough exploration of the existing methodologies for safety risk analysis and assessment and processes for management of engineering safety in railway industry. The author considered and commented on a substantial number of methodologies, tools and modelling techniques. The findings of this initial research are outlined in chapters two and three of the thesis. Following from there, the author used as vehicles a number of projects for further analyses and development of initial ideas as outlined in chapter 4.

the author identified a number of gaps, in particular in relation to establishment of a systems based framework for analysis, assessment and management of engineering

safety. These are discussed in chapter 5. As part of this work the author identified and discussed further the requirements for a new system based framework. The requirements framework has been structured to correspond to the number of stages within the safety risk analysis and management process.

The framework supports a system based approach to safety analysis and management and provides a complete step by step guidance for:

1. Conceptualisation of system supporting safety analysis;
2. Identification, analysis, assessment and management of safety risks;
3. Construction and management of safety cases.

the author successfully implemented and trialled this framework on two real life railway projects. Each of these stages is considered in turn and the findings presented here, with clear indication of fulfilment of the identified requirement and my contribution to wider knowledge and practice.

Additionally, the author analysed and further developed the theoretical background in relation to the concepts of “Hazard” and the “Safety case”.

8.1.2 The concepts of “Hazard” and the “Safety case”

the author analysed the hazard as a system concept and developed existing notions further, identified and defined the attributes, and their hierarchical structure, of a Hazard as a system.

the author analysed the concept of the safety case as the inquiry model identifying a number of constraints and requirements that a safety case must satisfy. Subsequent to analysis of these, the author proposed a general high level approach to structure of the safety case as a fact net, reasoning model.

This knowledge and understanding informed the later development of the engineering safety analysis and management process and methodologies.

CONTRIBUTION: knowledge and understanding of concepts such as “Hazard” and ”Safety Case” have been improved as part of this work.

8.1.3 Holistic Change Safety Analysis, Risk Assessment and Management Process

the author analysed the existing system safety and system engineering processes and guidance, and proposed a new framework. Firstly the author outlined the vision of the safety engineering as an integrated part of the system engineering process and the assurance of delivering the needed functioning of the four key emerging properties of any system: safety, RAM, Operability and Performance.

Following from that the author developed and outlined the integrated process for analysis and management of engineering safety. The process consist of 7 steps, most of which are not newly identified as needed but have not been formalised nor used together within an integrated framework.

As part of this research the author identified requirements for the integrated process, analysed existing methods and processes, identified gaps and outlined the need for a framework in chapter 4 of this thesis.

CONTRIBUTION: the new framework is now an integrated part of the Project Management Framework (PMF) for LU Upgrades Directorate and is known as Engineering Safety and Assurance Case (ESAC) and a process in supporting its delivery, Engineering Safety and Assurance Process (ESAP). A description of this and other engineering safety related deliverables and templates has been produced as part of the PMF (Lucic, 2009a), (Lucic, 2009b), (Lucic, 2009c), (Lucic, 2009d), (Lucic, 2009e).

As part of the initiative to implement the framework, training has been arranged (ESAC College) (Lucic, 2009f) and up to the date of issue of the thesis more than 150 engineers and managers from LU and the supply chain have been trained.

The author is the principle author of the course, with several other experts in the field contributing to the material through review and comments on an early version.

Step 1: System Conceptualisation, Representation and Scoping (System Analysis)

A number of methodologies for system conceptualisation have been analysed and some of these tested (chapters 2, 3 and 4). The author adopted the methodology initially developed by Short, “Process Models”, formalised it further and integrated it with the rest of the framework.

CONTRIBUTION: the author formalised the process and methodology for system conceptualisation within the general system safety framework and wider within the system engineering framework. the author developed further the existing concept of “process models” to enable development of the hierarchical conceptualisation models on real life projects as detailed in Chapters 6 and 7.

Step 2: Information processing

As indicated earlier the information processing can be structured in a number of activities. Following is a summary of the research findings and a contribution statement against each one of these activities.

Core hazard grouping, Hazard identification and Analysis of causalities and consequences

A two stage process, Initial Change Safety analysis and Change Safety Analysis has been developed and implemented. As depicted in Chapters 6 and 7.

CONTRIBUTION: the author performed a research and identified a set of the core hazards on real life projects. These have been distinctly defined and are being used at the core of the safety analysis and in support of structuring the safety cases across the project. the author defined and successfully applied a new holistic framework for safety analysis mainly by means of enhancing and formalising already existing processes such as structured hazard identification using guide words, FMEA techniques, use of process models, and integrating them together into a comprehensive framework.

the author made extensive use of the theoretical work the author completed in relation to the understanding of a concept of “Hazard” and its attributes from a system viewpoint.

Risk assessment

the author undertaken a review and analysis of existing risk assessment techniques. The author developed technique and methodology for integration of standalone QRA models into an integrated system risk model as well as the specification for software tool in support of the methodology. This work is outlined in Chapter 4, sections 1st and 2nd Project. Unfortunately, the results of this research (toolset) were not transferable across, onto the LU Upgrade projects for financial and IT service reasons.

the author developed a process that brings together the qualitative and quantitative risk assessment methodologies into a framework supporting the production of the safety case and the ALARP argument. This has been applied on the real life project (LU Upgrades) as depicted in Chapter 7. The quantified approach is used to set the safety targets and monitor safety performance of the railway throughout the migration whilst in support of the ALARP argument a comparative, qualitative, method is used.

CONTRIBUTION: the author developed and successfully trialled on a real life project, a new quantified risk assessment methodology. This work is described in Chapter 4, sections 1st and 2nd Project. New blend of the quantified and qualitative approach was developed and successfully applied on a LU Project as described in Chapter 7.

Estimation and apportionment of the safety risk to the source causes and failures of preventative measures and risk profiling

As part of the project depicted in Chapter 4, section 1st Project the author developed algorithms for calculation of the contribution of equipment and procedural failures and human errors to the total safety risk. This methodology was successfully applied on the project and used to establish the safety targets at the subsystem level for the new train control system. The same methodology was used to develop multidimensional risk profile.

As part of the LU Upgrade projects, the existing LU models have been utilised to define the system level hazard rates and calculate the contribution of the signalling system and rolling stock related failures to the overall risk.

CONTRIBUTION: the author developed new algorithms for apportionment and importance calculations within the cause-consequence QRA modelling environment. This has been successfully applied on a project.

A team of safety professionals under my guidance and following my instructions have implemented the framework the author developed for the QRA related work on the LU Upgrades. This work is depicted in Chapter 7.

Identification of different solutions and mitigation measures (options and impact analysis) and optimisation of the system and selection of most gainful options and mitigations

The outline of the need to undertake options and impact analysis is defined by industry standards and the legal framework in the UK. The author developed this framework further, combining the use of quantitative and qualitative analysis and assessment.

The numerical safety targets are set using quantified risk modelling. The impact of the achieved performance of the subsystems on the overall system safety performance is tested using the QRA.

The system level ALARP argument is supported by the ALARP review process developed by me using the existing comparative assessment criteria. As part of

this assessment, if there is a need for any further reduction of risk, different options are assessed and evaluated, taking in consideration all relevant parameters as defined with the framework.

CONTRIBUTION: the author improved some aspects of existing methodologies and developed a process for options analysis integral to the overall system safety management framework, implemented within the LU Upgrades.

Assertion of Completeness of System Analysis and Assessment of Uncertainties

the author analysed the problem of the completeness of the system analysis and uncertainty of information and data. The author identified four distinct areas where assurance for completeness and analysis of uncertainty is required.

CONTRIBUTION: For each one of these the author proposed and successfully implemented a framework in support of the assurance process and delivery of the related arguments and justification.

Step 3: Derivation and management of requirements

Existing well defined process for derivation of safety requirements have been followed and applied within the new framework. The author analysed the concept of the safety requirement from the system point of view and proposed a minor clarification of the definition and the topology of safety requirement as a system safety “object” in relation to defence/protection measures.

CONTRIBUTION: the author defined the attributes for safety requirements and integrated and applied existing processes into a new framework.

Step 4: Presentation of results and construction of safety knowledge net

the author briefly analysed the reporting requirements on in support of the safety related activities and have identified 5 different types of reports.

Of particular importance is the Safety Case. Complexity of modern systems inevitably brings about the intricacy of the safety case arguments or facts nets. Thus, it is necessary to endeavour to simplify the logic of the safety case fact net for a number of reasons:

1. To provide the focus assisting the experts involved in production of the safety case;
2. To assist the understanding aiding the reviewers;

3. To ease the management of updates and configuration control of the data and subsequently changes to the safety case.

A method of achieving these requirements, discussed earlier, has been implemented on both VLUP and SSL.

CONTRIBUTION: the author analysed the problem of complexity of constructing the fact net or a reasoning model in support of the safety argument and subsequent reporting, identified requirements for successful completion of it and proposed and implemented a structured approach to development of the safety case. This approach has been turned into a template and is now an integral part of the LU Upgrades processes and the Project Management Framework (Lucic, 2009a), (Lucic, 2009b), (Lucic, 2009c), (Lucic, 2009d), (Lucic, 2009e).

Step 5: Management support

In addition to usual project management related activities, management of the hazard logs, operational restrictions and the safety case delivery is necessitated as part of the engineering safety management activity.

Regarding a hazard log as a tool for Change Safety Management, Configuration Control and Reporting, the author analysed the problem domain from the system analysis perspective, identified requirements and defined the data model (hierarchy and topology) for the hazard log.

With regards to management of operational restrictions, the author analysed the problem domain, identified the process requirements and defined the template for the restrictions register.

Finally, with regards to the management of the safety case delivery, as part of the overall framework the author identified the requirements and defined the processes supporting this activity including an outline template of a remit document.

For all reports associated with the above activities the author identified requirements and defined the template and context including means of measuring progress.

CONTRIBUTION: the author implemented all of the above processes and methods on real life projects and integrated these into an overall system safety management process.

Step 6: Configuration control

As integral part of the research the author identified the configurable data items, defined the hierarchy and topology of these and defined the requirements for configuration management of these data. In completing this work the author used

guidance from the industry standards, which provide a high level outline of basic needs for configuration management but do not provide the detail.

CONTRIBUTION: the author implemented the configuration regime described as part of the overall system safety management process on the LU Upgrades.

Step 7: Continual appraisal and knowledge update

Apart from implementing existing guidance as part of the system safety management process framework the author did no further work in this area.

8.1.4 Overall contribution

The author defined and successfully implemented a novel framework for system safety management on large projects. The framework has been accepted by LU Upgrades and is formalised through a number of procedures and the Project Management Framework (Lucic, 2009a), (Lucic, 2009b) , (Lucic, 2009c), (Lucic, 2009d) , (Lucic, 2009e) ,.

As part of the initiative to implement the new Engineering Safety and Assurance Case framework across the LU Upgrades, the author developed and delivered training course (ESAC College) (Lucic, 2009f) to close to 120 professionals.

The author published a number of papers and delivered several lectures on this subject ((Lucic and Short, 2007), (Regan and Lucic, 2008), (Lucic, 2008), (Lucic, 2005a), (Lucic, 2005b)) at IEEE, IET, INCOSE seminars and as part of the Risk Management module of the MSc in Energy and Environmental Technology & Economics Module at City University.

8.2 Future Work

The system safety analysis and management framework that the author developed has been implemented and is proved in anger.

Dissemination of the good practice within LU continues with “ESAC College” being used as a vehicle and attendance to it being mandatory to project engineers and managers.

As part of continuous development and improvement policy the author embedded within the team we are challenging the framework process and the methodologies as well as deliverables. The change control process is established and in case that a weakness in the process or omission within any of the deliverables is identified an immediate action is taken to identify and implement correction

Most of the methodologies used within the framework are supported by tools; however a tool that could support and automate the integration of the methodologies would be extremely beneficial. At the moment this facility is embedded within the hazard log database but the process of cross-referencing the hazard constituents to originating process models interfaces, QRA elements, safety requirements repository, GSN elements, related documents, etc is manual, time consuming and prone to human error.

Some of these facilities are provided in the Integrated Safety Assurance Network (link between the QRA and Hazard log and documents register) so the logical step forward would be to utilise and extend capabilities of the ISAE tool.

The author is working on development of a specification and subsequently a business case for development of a tool (or a toolset) that would provide the following capabilities within the same environment:

1. Process modelling tool:
 - a. GUI with symbols tool set;
 - b. Object and interfaces database (object and interfaces created and information populated via GUI);
 - c. Facility to call up hazard log user interface from an object or interface symbol , automatically passing cross referencing information to newly created hazard log record and establishing a link between the two data sets;
 - d. Reporting;
2. Hazard log with functionalities described earlier has already been developed. However following functionalities should be added:
 - a. Real time aligning and parallel working with the Process Modelling environment;
 - b. Automatic generation of the “hazard universe” graphical metta model as support to analysis of its structure, constituents and topology;
 - c. Automated linkage to requirements management tools (DOORS for example) enabling automatic cross referencing and tracking of progress;
3. Quantitative and Qualitative Risk Assessment. A tool that provides most of the functionalities for qualitative and quantitative risk assessment with some

linkage to the hazard log already exist, ISAE tool delivers some of the functionality required to support the framework. Further enhancements are necessary as follows:

- a. Automatic linkage between the “hazard universe” constituents and Quantitative and Qualitative Risk Assessment data constituents;
4. GSN generation tool. The author believes that it is possible to automate generation of a draft GSN using the structured information in the hazard log. This GSN could only ever be used as a draft for detailed review, but creation of a real-time link between the “hazard universe” constituents and the safety case arguments-evidence net would be extremely valuable supporting reviews and sense check as well as enabling automatic synchronisation between the hazard log (and through hazard log the process models, QRA, Requirements, Restrictions, actions management and the safety case.

A railway system is a “System of Systems” (SoS) (Karcantias and Hessami, 2008) and (Karcantias and Hessami, 2008). As the theory of SoS advances, the process outlines in this thesis needs to be kept aligned with the latest developments.

A particular limitation of the process is related to lack of temporal properties of process models. Further development of process models methodology to cater better for temporal properties of the system, improving the identification and analysis of emerging properties of complex systems, is a challenge that would be worth taking on.

Initial results from a number of case studies in different industries indicate that further research and refinement into the area of justifiable spend, and extension of the research into J-value, carried out by Thomas and Stupples (Thomas and Stupples, 2006), to incorporate societal perception of risk acceptance will be beneficial.

CHAPTER 9: REFERENCES AND BIBLIOGRAPHY

- (ATKINS, 2002) ATKINS GLOBAL (2002) *Axle Counter Concept Safety Case*, London: ATKINS GLOBAL (Reference 1956007-L-SC-001, v7.00, dated 22-03-2002).
- (ATKINS, 2003) ATKINS GLOBAL (2003) *Systems Integration*; London: ATKINS GLOBAL (Reference 5012008-51-001 Issue 1; 28/11/2003).
- (Bernstein, 1996) Bernstein P. L. (1996) *Against the Gods: Remarkable Story of Risk*. USA: John Wiley & Sons, INC; ISBN-471-29563-9.
- (Bhatnagar and Kanal, 1991) Bhatnagar R. and Kanal N. L. (1991) *Models of enquiry and formalism for approximate reasoning*; USA: University of Maryland College Park.
- (Blanchard and Fabrycky, 1998) Benjamin S. Blanchard and Wolter J. Fabrycky (1998) *Systems Engineering and Analysis*. New Jersey: Prentice-Hall, Inc. ISBN 0-13-135047-1.
- (Bobbio and Portinali, 1999) Andrea Bobbio and Luigi Portinali (1999) Comparing different methodologies of Probabilistic Structured Modelling by the analysis of typical industrial dependable systems. *CENELEC WGA10 Workshop: Bridging the Gap to Railway Interoperability*, Germany, Munich.
- (BS EN 50126: 1999) BRITISH STANDARDS INSTITUTE (1999) *Railway Applications – The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS)* London: British Standards Institute.
- (BS EN 50129, 2003) BRITISH STANDARDS INSTITUTE (2003) *Railway Applications: Software for Railway Control and Protection Systems*. London: British Standards Institute. ISBN 0 580 41814 6.
- (BS EN 61508: 2003) BRITISH STANDARDS INSTITUTE (2003) *Functional Safety of electrical/electronic/programmable electronic safety-related systems* London: British Standards Institute.
- (CENELEC 1998) CENELEC (1998) *TC9XA-WGA10- A Method for SIL Allocation*. EU: CENELEC.
- (CENELEC 2003) CENELEC EN (2003) *50129: Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*. EU: CENELEC.
- (Checkland, 1984) Checkland P. (1984) *Systems Thinking Systems Practice*. England: John Wiley & Sons Ltd; ISBN 0-471-27911-0.

- (Civil Aviation Authority, 2006) CIVIL AVIATION AUTHORITY (2006) *CAP 760 Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases For Aerodrome Operators and Air Traffic Service Providers*. UK: Safety Regulation Group.
- (Fenton and Hill, 1993) Fenton N. and Hill G. (1993) *Systems Construction and Analysis, A Mathematical and Logical Framework*. London: McGraw-Hill Book Company Europe, ISBN 0-07-707431-9.
- (Fenton, 1991) Fenton N. (1991) *Software Metrics – A Rigorous Approach*. London: Chapman and Hall, ISBN 0-412-40440-0.
- (Fenton, Neil and Forey, 2001) Fenton N. , Neil M., Forey S. and Harris R. (2001) Using BBNs to predict the reliability of military vehicles. *Computing and control engineering journal*; pp 11-20.
- (Fragola and Spahn, 1973) Fragola, J.R. and Spahn J.F. (1973), The Software Error Effects Analysis; A Qualitative Design Tool, In: *Proceedings of the 1973 IEEE Symposium on Computer Software Reliability*, IEEE, New York, pp. 90-93
- (Goble, 1998) Goble W. M. (1998) *The use and development of quantitative reliability and safety analysis in new product design*, PhD), Technische Universiteit Eindhoven, ISBN 60-386-0870-5.
- (Health and Safety Executive, 2001) GREAT BRITAIN. HEALTH AND SAFETY EXECUTIVE (2001) *Reducing risks, protecting people*. London: Her Majesty's Stationery Office ISBN 0717621510
- (Health & Safety Commission, 1998) GREAT BRITAIN. HEALTH AND SAFETY COMMISSION (1998) *Rail Safety: Proposal for Regulations on train protection systems and mark 1 stock (Consultative Document)*. London. HSE Books.
- (Hessami 2004) Hessami, A., (2004) A systems framework for Safety and Security: the holistic paradigm. *Systems Engineering*; Volume 7; ISSN 1098-1241.
- (Hessami and Hunter, 2002) Hessami A. and Hunter A. (2002) Formalization of weighted factors analysis, *Knowledge-Based Systems*, Issue 15, pp. 377-390.
- (Hessami, 1999a) Hessami, A. (1999) Risk, a Missed Opportunity. *Risk & Continuity-The International Journal for Best Practice Management*, Volume 2, Issue2.
- (Hessami, 1999b) Dr Ali Hessami, (1999) Risk Management: A Systems Paradigm. *Systems Engineering*, Volume 2, Number 3.

- (Hsu and Musicki, 2005) Feng Hsu and Zoran Musicki (2005) Issues and Insights of Probabilistic Risk Assessment Methodology in Nuclear and Space Applications. In: *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, ISBN: 0-7803-9298-1.
- (Karcanias and Hessami, 2009) Karcanias N. and Hessami A. (2008) *Complexity and the Notion of System of Systems: Part (I): General Systems and Complexity*; Unpublished paper, City University, London.
- (Karcanias and Hessami, 2009) Karcanias N. and Hessami A. (2008) *Complexity and the Notion of System of Systems: Part (II): Defining the notion of System of systems*; Unpublished paper, City University, London.
- (Karcanias, 2003) Karcanias N (2003) *System Concepts for General Processes: Specification of a New Framework*. Unpublished paper, City University, London.
- (Karcanias, 2004) Karcanias N (2004) Complex Systems: Modelling and Simulation Challenges. *SIM-SERV workshop: Working Group on Modelling and Simulation* Greece, University of Patras.
- (Kelly and Weaver, 2004) Kelly T. and Weaver R. (2004) The Goal Structuring Notation – A Safety Argument Notation. In: *Proceedings of Dependable Systems and Networks 2004 Workshop on Assurance Cases*. UK.
- (Kelly, 2001) Contract Research Report for QinetiQ COMSA/2001/1/, Kelly, T. (2001) *Concepts and Principles of Compositional Safety Case Construction*. York: Department of Computer Science, University of York.
- (Kirwan, 1996) Barry Kirwan (1996) The validation of 3 Human Reliability Quantification techniques – THERP, Heart and JHDI, *Applied Ergonomics* Vol. 27. No 6pp.359-373.
- (Linstone and Turoff , 2002) Linstone H. A. and Turoff M.(2002) *The Delphi Method: Techniques and Applications*. New Jersey, New Jersey Institute of Technology.
- (Lucic and Short, 2007) Lucic I. and Short R. (2007) Engineering Safety and Assurance Case. In: *Proceedings of the Institution of Engineering and Technology Seminar on Safety Assurance, 7 – 8 November 2007*. London.
- (Lucic, 2001) ATKINS RAIL REPORT- Lucic I. (2001) *Proposal for development of methodology for risk based application of TPWS to speed restriction, Version 01*. London.
- (Lucic, 2002) ATKINS RAIL REPORT- Lucic I. (2002) *Manchester South Capacity Improvement Project: Hazard Forum Procedure (4026002-L-RM-004; Version 3.00; 25/11/2002)*. London.

- (Lucic, 2003a) ATKINS RAIL REPORT- Lucic I. (2003) *Axle Counter Risk Analysis* (Reference ET-JWR-010033541). London.
- (Lucic, 2003b) ATKINS RAIL REPORT- Lucic I. (2003) *Axle Counter – Modelling Enhancements, High Level Hazard Identification Report* (Reference 1956710-L-HA-001, version 00.04, dated 09-01-2003). London.
- (Lucic, 2003c) ATKINS RAIL REPORT- Lucic I. (2003) *Stage 1 - Test Plan*, (Reference 195620-L-TG-001, version 1.0, dated 14/05/03). London.
- (Lucic, 2003d) ATKINS RAIL REPORT- Lucic I. (2003) *Manchester South Capacity Improvement Project: Change safety analysis Strategy (FF05-000-SA-SAC-5204.v04.00; 31/10/03)*. London.
- (Lucic, 2004a) ATKINS RAIL REPORT- Lucic I. (2004) *Axle Counter Modelling - Stage 1 Final Report* (Reference 1956710-L-TR-001 issue 01.00). London.
- (Lucic, 2004b) ATKINS RAIL REPORT- Lucic I. (2004) *Manchester South Capacity Improvement Project: Hazard Management Plan (FF05-000-SA-SAC-5004.v06.00; 24/05/2004)*. London.
- (Lucic, 2005a) Lucic I. (2005) *Holistic Safety Performance Forecasting For Train Detection System*. In: *Proceedings of the System of Systems Engineering, IEEE-International Conference on Systems, Man and Cybernetics October 10-12, 2005*. USA, Hawaii.
- (Lucic, 2005b) Lucic I. (2005-2010) Lectures “Risk Profiling: a Strategic Instrument” and “Engineering Safety and Assurance”, *Delivered at: City University as part of the Risk Management module of the MSc in Energy and Environmental Technology & Economics Module*. UK, London.
- (Lucic, 2005c) RAILTRACK REPORT – Lucic I. (2005) *ERTMS Hazard identification and grouping report*. London
- (Lucic, 2005d) RAILTRACK REPORT – Lucic I. (2005) *ERTMS QRA model and the report*. London.
- (Lucic, 2005e) RAILTRACK REPORT – Lucic I. (2005) *ISAE Enhancements specification*. London.
- (Lucic, 2005f) RAILTRACK REPORT – Lucic I. (2005) *ERTMS Safety Targets – report*. London.
- (Lucic, 2006) ATKINS RAIL REPORT- Lucic I. (2006) *Technical Assistance for Preparation of the Modernisation of Corridor II – Remaining Works-Development of System Description & RAMS Requirements Strategy; 24th May 2006; (Minutes of Meeting)*. London.

- (Lucic, 2008) Lucic I. (2008) Lecture “Engineering Safety and Assurance Case (ESAC)”;
Delivered at: The IET Course on Railway Signaling and Control Systems 2008. UK, Birmingham.
- (Lucic, 2009a) LONDON UNDERGROUND REPORT – Lucic I. (2009) *Project Management Framework Product Description and Template: Engineering Safety Management Plan (LU-PD-10655 A1)*. London.
- (Lucic, 2009b) LONDON UNDERGROUND REPORT – Lucic I. (2009) *Project Management Framework Product Description and Template: Engineering Safety Case (LU-PD-10656 A)*. London.
- (Lucic, 2009c) LONDON UNDERGROUND REPORT – Lucic I. (2009) *Project Management Framework Product Description and Template: Engineering Safety & Assurance Case (ESAC) Case (LU-PD-10685 A1)*. London.
- (Lucic, 2009d) LONDON UNDERGROUND REPORT – Lucic I. (2009) *Project Management Framework Product Description and Template: Engineering Safety Hazard Log (LU-PD-10808 A1)*. London.
- (Lucic, 2009e) LONDON UNDERGROUND REPORT – Lucic I. (2009) *Project Management Framework Product Description and Template: System Safety Case (LU-PD-10739 A1)*. London.
- (Lucic, 2009f) LONDON UNDERGROUND REPORT – Lucic I. (2009) *ESAC College Notes (GEN-9999-LUL-ESAC-00001)*. London.
- (Ludwig, 2005) Dr. Ing. habil. Bjorn Ludwig (2005) Safety management systems-a new challenge for railways? *ETR. Eisenbahntechnische Rundschau*, vol. 53, no11, pp. 749-757. ISSN 0013-2845.
- (Milloti, 2004) Dia Milloti (2004) *Systems, modelling and control in manufacturing and business processes* (PhD Transfer report) City University – London.
- (Moss and Woodhouse, 1999) Moss T. R. and Woodhouse J. (1999) Criticality Analysis Revisited. *Quality and Reliability Engineering International*, Volume 15, Issue 2, pp.117-121.
- (Open University Handbook, 1999) The Open University (1999) *Mathematical Methods, Models and Modelling-Handbook*. UK: OU; SUP 46655 8, 1999.
- (Portland and Turoff, 2002) Harold A. Linstone Portland and Murray Turoff (2002) *The Delphi Method - Techniques and Applications*. New Jersey: New Jersey Institute of Technology; University of Southern California, ISBN 0-201-04294-0.

- (Pukite and Pukite, 1998) Pukite J. and Pukite P. (1998) *Modelling for Reliability Analysis*; US: Wiley-IEEE Press, ISBN 0-7803-3482-5.
- (Regan and Lucic, 2008) Regan L. and Lucic I. (2008) Use of QRA in Supporting a System Safety Case for the Victoria Line Upgrade. In: *Proceedings of the INCOSE 18th Annual International Symposium 2008, System Engineering for the Planet*. The Netherlands, Utrecht.
- (Reifer, 1979) Reifer D.J. (1979) Software Failure Modes and Effects Analysis. *IEEE Transactions on Reliability*, Vol. R-28, No. 3.
- (Rouvroye, 2001) Rouvroye J. L. (2001) *Enhanced Markov Analysis as a method to assess safety in the process industry* (PhD), Technische Universiteit Eindhoven, ISBN 90-386-2772-6.
- (RSSB, 2007) UNITED KINGDOM. RAIL SAFETY AND STANDARDS BOARD on behalf of the UK Rail Industry (2007) *Engineering Safety Issue 3 - Yellow book*. London: RSSB; ISBN 0 9537595 0 4.
- (Russo and Jain, 2001) Russo M. and Jain L.C. (2001) *Fuzzy Learning and Applications* New York: CRC Press, ISBN 0-8493-2269-3
- (Saltelli, 2002) Andrea Saltelli (2002) Sensitivity analysis for importance assessment; *Risk Analysis: an official publication of the Society for Risk Analysis*.
- (SAMRAIL, 2004) European Commission Fifth Framework Programme – SAMRAIL-Consortium (2004) *Common Safety Methods, Version 3*. London: ATKINS GLOBAL.
- (Short, 2007) Short R. (2007) Combining Different Types of Evidence in System Safety Assurance. In: *SARAC Asia Pacific Transport Safety & Security Conference*. China, Beijing.
- (Short, 2009) Short R. (2009) The Use and Misuse of SIL; *IET/IRSE Technical Meeting*. London: IRSE.
- (Sterman, 2000) Sterman J. D. (2000) *Business Dynamics – Systems Thinking and Modelling for a Complex World*. US: Irwin McGraw-Hill I. ISBN 0-07-231135-5.
- (Thomas and Stupples, 2006) Thomas P. J. and Stupples D. W. (2006) J Value: a universal scale for health and safety spending. *Measurement + Control*; Vol.39/9 pp. 273-276.
- (Topintzi, 2001) Topintzi E. (2001) *System Concepts and Formal Modelling Methods for Business Processes* (PhD), City University – London.
- (Waldrop, 1992) Waldrop M. M. (1992) *Complexity, the emerging science at the edge of order and chaos*. New York: Simon & Schuster Paperback; ISBN 0-671-76789-1

- (Waring, 1996) Alan Waring (1996) *Practical System Thinking*. International Thomson Business Press, ISBN 0-412-71750-6.
- (Department of Transport, 1989) GREAT BRITAIN. DEPARTMENT OF TRANSPORT (1989), *Investigation into the Clapham Junction Railway Accident (Anthony Hidden QC)*. London. Her Majesty's Stationery Office, ISBN 0 10 1082029.

Papers and Reports published by author of the thesis

- (Lucic and Short, 2007) Lucic I. and Short R. (2007) *Engineering Safety and Assurance Case*. In: *Proceedings of the Institution of Engineering and Technology Seminar on Safety Assurance, 7 – 8 November 2007*. London.
- (Lucic, 2001) ATKINS RAIL REPORT- Lucic I. (2001) *Proposal for development of methodology for risk based application of TPWS to speed restriction, Version 01*. London.
- (Lucic, 2002) ATKINS RAIL REPORT- Lucic I. (2002) *Manchester South Capacity Improvement Project: Hazard Forum Procedure (4026002-L-RM-004; Version 3.00; 25/11/2002)*. London.
- (Lucic, 2003a) ATKINS RAIL REPORT- Lucic I. (2003) *Axle Counter Risk Analysis* (Reference ET-JWR-010033541). London.
- (Lucic, 2003b) ATKINS RAIL REPORT- Lucic I. (2003) *Axle Counter – Modelling Enhancements, High Level Hazard Identification Report* (Reference 1956710-L-HA-001, version 00.04, dated 09-01-2003). London.
- (Lucic, 2003c) ATKINS RAIL REPORT- Lucic I. (2003) *Stage 1 - Test Plan*, (Reference 195620-L-TG-001, version 1.0, dated 14/05/03). London.
- (Lucic, 2003d) ATKINS RAIL REPORT- Lucic I. (2003) *Manchester South Capacity Improvement Project: Change safety analysis Strategy (FF05-000-SA-SAC-5204.v04.00; 31/10/03)*. London.
- (Lucic, 2004a) ATKINS RAIL REPORT- Lucic I. (2004) *Axle Counter Modelling - Stage 1 Final Report* (Reference 1956710-L-TR-001 issue 01.00). London.
- (Lucic, 2004b) ATKINS RAIL REPORT- Lucic I. (2004) *Manchester South Capacity Improvement Project: Hazard Management Plan (FF05-000-SA-SAC-5004.v06.00; 24/05/2004)*. London.

- (Lucic, 2005a) Lucic I. (2005) Holistic Safety Performance Forecasting For Train Detection System. In: *Proceedings of the System of Systems Engineering, IEEE-International Conference on Systems, Man and Cybernetics October 10-12, 2005*. USA, Hawaii.
- (Lucic, 2005b) Lucic I. (2005-2010) Lectures “Risk Profiling: a Strategic Instrument” and “Engineering Safety and Assurance”, *Delivered at: City University as part of the Risk Management module of the MSc in Energy and Environmental Technology & Economics Module*. UK, London.
- (Lucic, 2005c) RAILTRACK REPORT – Lucic I. (2005) *ERTMS Hazard identification and grouping report*. London
- (Lucic, 2005d) RAILTRACK REPORT – Lucic I. (2005) *ERTMS QRA model and the report*. London.
- (Lucic, 2005e) RAILTRACK REPORT – Lucic I. (2005) *ISAE Enhancements specification*. London.
- (Lucic, 2005f) RAILTRACK REPORT – Lucic I. (2005) *ERTMS Safety Targets – report*. London.
- (Lucic, 2006) ATKINS RAIL REPORT- Lucic I. (2006) *Technical Assistance for Preparation of the Modernisation of Corridor II – Remaining Works-Development of System Description & RAMS Requirements Strategy; 24th May 2006; (Minutes of Meeting)*. London.
- (Lucic, 2008) Lucic I. (2008) Lecture “Engineering Safety and Assurance Case (ESAC)”; *Delivered at: The IET Course on Railway Signaling and Control Systems 2008*. UK, Birmingham.
- (Lucic, 2009a) LONDON UNDERGROUND REPORT – Lucic I. (2009) *Project Management Framework Product Description and Template: Engineering Safety Management Plan (LU-PD-10655 A1)*. London.
- (Lucic, 2009b) LONDON UNDERGROUND REPORT – Lucic I. (2009) *Project Management Framework Product Description and Template: Engineering Safety Case (LU-PD-10656 A)*. London.
- (Lucic, 2009c) LONDON UNDERGROUND REPORT – Lucic I. (2009) *Project Management Framework Product Description and Template: Engineering Safety & Assurance Case (ESAC) Case (LU-PD-10685 A1)*. London.
- (Lucic, 2009d) LONDON UNDERGROUND REPORT – Lucic I. (2009) *Project Management Framework Product Description and Template: Engineering Safety Hazard Log (LU-PD-10808 A1)*. London.

- (Lucic, 2009e) LONDON UNDERGROUND REPORT – Lucic I. (2009) *Project Management Framework Product Description and Template: System Safety Case (LU-PD-10739 A1)*. London.
- (Lucic, 2009f) LONDON UNDERGROUND REPORT – Lucic I. (2009) *ESAC College Notes (GEN-9999-LUL-ESAC-00001)*. London.
- (Regan and Lucic, 2008) Regan L. and Lucic I. (2008) Use of QRA in Supporting a System Safety Case for the Victoria Line Upgrade. In: *Proceedings of the INCOSE 18th Annual International Symposium2008, System Engineering for the Planet*. The Netherlands, Utrecht.

APPENDIX A: ALGORITHMS FOR APPORTIONMENT AND IMPORTANCE IN CAUSE-CONSEQUENCE MODELS

Apportionment of a virtual consequence to lower level virtual consequences

Apportionment of virtual consequence to the lower level virtual consequence is calculated as a proportion of the Risk contributed to the virtual consequence by the lower layer virtual consequence. Therefore, if R_{vj}^l is a risk of the virtual consequence 'j' ($1 \leq j \leq n$) at level 'l' ($1 \leq l \leq n$), then,

$$R_{vj}^l = \sum_{i=1}^{i=n} R_{vi}^{l-1} \quad \text{Equation 5}$$

Hence, the fractional contribution of the virtual consequence 'x' ($1 \leq x \leq n$) at lower level 'l-a' ($1 \leq l \leq n$; $1 \leq a \leq n$; $l > a$) to the virtual consequence 'j' ($1 \leq j \leq n$), at level 'l' equals to:

$${}_{vj}A_{vx}^{l-a} = \frac{R_{vx}^{l-a}}{R_{vj}^l} = \frac{R_{vx}^{l-a}}{\sum_{i=1}^{i=n} R_{vi}^{l-a}} \quad \text{Equation 6}$$

Where:

R_{vx}^{l-a} Is a risk of the lower level virtual consequence 'x' ($1 \leq x \leq n$), at level 'l-a' whose contribution is calculated.
 R_{vj}^l Is a risk of the virtual consequence 'j' at level 'l' analysed.

Apportionment of a virtual consequence to "source" consequences

"Source" consequences are consequences arising directly from the model before any grouping has taken a place.

If R_{vj}^l is a risk of the virtual consequence 'j' at any level 'l' and ${}_{vj}R_{si}^{cek}$ is a risk of any "source" consequence 'i' ($1 \leq i \leq n$), arising from any Critical Event 'k' ($1 \leq k \leq n$) and feeding the virtual consequence 'j', then,

$$R_{vj}^l = \sum_{k=1}^{k=n} \sum_{i=1}^{i=n} {}_{vj}R_{si}^{cek} \quad \text{Equation 7}$$

Where:

$\sum_{k=1}^{k=n} \sum_{i=1}^{i=n} {}_{vj}R_{si}^{cek}$ Is a total of risk of all source consequences 'i' arising from different Critical Events 'k'

Hence, the fractional contribution of the "source" consequence 'y', arising from the Critical Event 'h' and feeding the virtual consequence 'j', to the virtual consequence

'j' at any level 'l' equals to:

$${}_{vj}A_{sy} = \frac{{}_{vj}R_{sy}^{ceh}}{R_{vj}^l} = \frac{{}_{vj}R_{sy}^{ceh}}{\sum_{k=1}^{k=n} \sum_{i=1}^{i=n} {}_{vj}R_{si}^{cek}} \quad \text{Equation 8}$$

Where:

${}^{vj}R_{sy}^{ceh}$	Is the risk of a “source” consequence ‘y’ whose contribution is calculated.
R_{vj}^l	Is a risk of the virtual consequence ‘j’ at any level ‘l’ analysed.

Apportionment of a virtual consequence to Core Hazards (Critical Events)

Risk arising from the Core Hazard (Critical Event) is equal to a total of risks embodied within all the “source” consequences arising from the Core Hazard. However, contribution of a Core Hazard to a Virtual Consequence equals to a sum of risks embodied within only those “source” consequences originating from the Core Hazard which are grouped into the Virtual Consequence analysed. Therefore ${}^{vj}A_{ceh}$, fractional contribution of the Critical Event ‘h’ ($1 \leq h \leq n$) to the virtual consequence ‘j’ at level ‘l’ equals to:

$${}^{vj}A_{ceh} = \frac{\sum_{i=1}^{i=n} {}^{vj}R_{si}^{ceh}}{\sum_{k=1}^{k=n} \sum_{i=1}^{i=n} {}^{vj}R_{si}^{cek}} \quad \text{Equation 9}$$

Where:

$\sum_{i=1}^{i=n} {}^{vj}R_{si}^{ceh}$	Is the sum of risks of all the “source” consequences ‘i’ arising from the critical event ‘h’ feeding into a virtual consequence ‘j’.
$\sum_{k=1}^{k=n} \sum_{i=1}^{i=n} {}^{vj}R_{si}^{cek}$	Is the sum of risks of all the “source” consequences ‘i’ arising from all critical events ‘k’ ($1 \leq k \leq n$) feeding into a virtual consequence ‘j’.

Importance of Base Events relative to a “source” consequence or a virtual consequence

In order to define the contributions from base events to the consequences, decision was made to use the Fussel-Vesely (FV) importance value. Fussel-Vesely importance is a measure of the contribution a constituent of the fault tree makes to the top event probability or frequency. It is defined as the sum of the probabilities or frequencies of all cutsets in which the constituent appears, divided by the top event probability or frequency. This value is sometimes referred to as Fractional Importance. In effect the Fussel-Vesely importance is a measure of the sensitivity of the top event to changes in the base event. Fractional importance of the Base Event ‘x’ ($1 \leq x \leq n$) to the Critical Event (Hazard) ‘k’ regarding Fussel-Vesely value is then given by:

$${}^{cek}I_{bex} = \frac{FV_{bex}}{\sum_{i=1}^{i=n} FV_{bei}} \quad \text{Equation 10}$$

Where:

FV_{bex} Is the Fussel-Vesely importance value for the Base Event 'x'.

$\sum_{i=1}^{i=n} FV_{bei}$ Is the total Fussel Vesely importance value of the model (sum of FV values of all Base Events 'i' within the model).

Fractional importance of the Base Event 'x' ($1 \leq x \leq n$) to the "source" consequence 'y', originating from Critical Event 'h', regarding Fussel-Vesely value is same as the Fractional importance of the Base Event 'x' ($1 \leq x \leq n$) to the Critical Event (Hazard) 'h' giving a rise to the "source" consequence 'y' and is given by:

$${}_{sy}I_{bex}^{ceh} = {}_{bex}I_{bex}^{ceh} = \frac{FV_{bex}}{\sum_{i=1}^{i=n} FV_{bei}} \quad \text{Equation 11}$$

Where:

FV_{bex} Is the Fussel Vesely importance value for the Base Event 'x'.

$\sum_{i=1}^{i=n} FV_{bei}$ Is the total Fussel Vesely importance value of the model (sum of FV values of all Base Events 'i' within the model).

Fractional importance of the Base Event 'x' ($1 \leq x \leq n$) to the virtual consequence 'j' at any level 'l', regarding Fussel-Vesely value, is relative to the fractional contribution of the "source" consequence 'y' ($1 \leq y \leq n$), originating from Critical Event 'h', the base event 'x' is causing, to the virtual consequence 'j' at any level 'l'. Therefore:

$${}_{vj}I_{bex} = {}_{sy}I_{bex}^{ceh} \cdot {}_{vj}A_{sy}^{ceh} = \frac{FV_{bex}}{\sum_{i=1}^{i=n} FV_{bei}} \cdot \frac{{}_{vj}R_{sy}^{ceh}}{R_{vj}^l} = \frac{FV_{bex}}{\sum_{i=1}^{i=n} FV_{bei}} \cdot \frac{{}_{vj}R_{sy}^{ceh}}{\sum_{k=1}^{k=n} \sum_{i=1}^{i=n} {}_{vj}R_{si}^{cek}} \quad \text{Equation 12}$$

Where:

${}_{vj}I_{bex}$ Is the Fractional importance of the Base Event 'x' ($1 \leq x \leq n$) to the virtual consequence 'j'.

${}_{sy}I_{bex}^{ceh}$ Is the Fractional importance of the Base Event 'x' ($1 \leq x \leq n$), causing a Critical Event 'h' to the "source" consequence 'y'.

${}_{vj}A_{sy}^{ceh}$ Is the fractional contribution of the "source" consequence 'y' ($1 \leq y \leq n$), arising from the Critical Event 'h', to the virtual consequence 'j' at any level 'l'.

FV_{bex} Is the Fussel-Vesely importance value for the Base Event 'x'.

$\sum_{i=1}^{i=n} FV_{bei}$ Is the total Fussel-Vesely importance value of the model (sum of FV values of all Base Events 'i' within the model).

${}_{vj}R_{sy}^{ceh}$ Is risk of the "source" consequence 'y', arising from the Critical Event 'h'.

R_{vj}^l Is a risk of the virtual consequence 'j' at any level 'l' analysed.

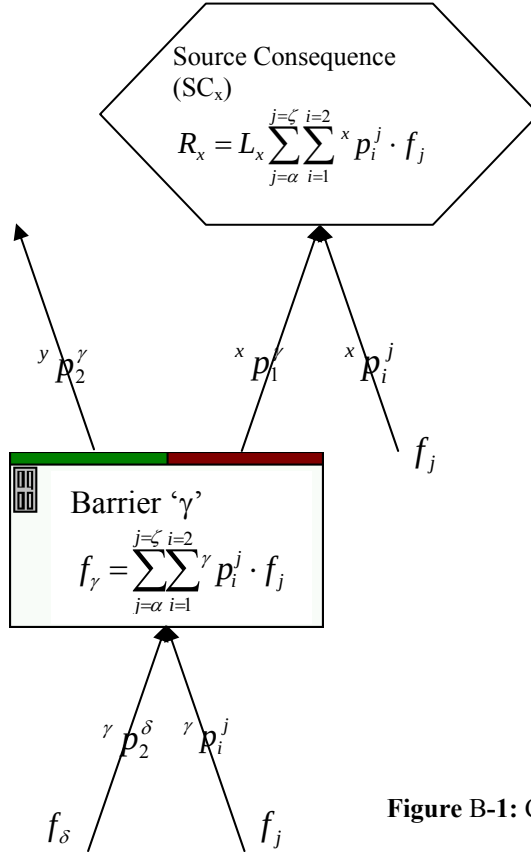
$\sum_{k=1}^{k=n} \sum_{i=1}^{i=n} v_j R_{si}^{cek}$ Is the sum of risks of all the “source” consequences ‘i’ arising from all critical events ‘k’ ($1 \leq k \leq n$) feeding into a virtual consequence ‘j’.

Importance of Barriers and Splitters relative to a “source” consequence or a virtual consequence

Measure of apportionment (importance) of the Barrier or Splitter is a measure of its “capability” to convey the frequency or probability of consequence occurrence towards the lower loss consequence.

For any consequence model element ‘j’ ($\alpha \leq j \leq \zeta$), frequency at the consequence model element, f_j , equals to a sum of all the frequencies feeding into the consequence model element ‘j’. Frequency coming out of the consequence model element is defined as a product of frequency at the consequence model element and probability of the consequence model element output.

Note: Consequence model element can be a barrier, a splitter or a critical event.



Therefore frequency at the consequence model element ‘ γ ’ is:

$$f_\gamma = \sum_{j=\alpha}^{j=\zeta} \sum_{i=1}^{i=2} \gamma p_i^j \cdot f_j \quad \text{Equation 13}$$

Where:

- f_γ Is the frequency at the consequence model element ‘ γ ’.
- γp_i^j Is the probability of any output ‘i’ of any consequence model element ‘j’ feeding into the consequence model element ‘ γ ’.
- f_j Is the frequency at any consequence model element ‘j’, whose output ‘i’ is feeding into the consequence model element ‘ γ ’.

Figure B-1: Consequence model notation

It follows that Risk of a “source” Consequence ‘x’ is a product of the Loss of the consequence and the sum of all the frequencies feeding into the consequence.

Therefore:

$$R_x = L_x \sum_{j=\alpha}^{j=\zeta} \sum_{i=1}^{i=2} x p_i^j \cdot f_j \quad \text{Equation 14}$$

Where:

R_x Is a risk of the “source” consequence ‘x’.
 L_x Is a loss of the “source” consequence ‘x’.
 ${}^x p_i^j$ Is probability of any output ‘i’ of any consequence model element ‘j’ feeding into the “source” consequence ‘x’.
 f_j Is the frequency at any consequence model element ‘j’, whose output ‘i’ is feeding into “source” consequence ‘x’ analysed.
 ‘Weight’ of a consequence model element’s output or risk conveyed through an output ‘i’ of a model element ‘j’ to a “source” consequence ‘x’ or the next consequence model element ‘x’ is equal to:

$$Wr_i^j = L_x \cdot {}^x p_i^j \cdot f_j \quad \text{Equation 15}$$

Where:

L_x Is a loss of the “source” consequence ‘x’ or the next consequence model element ‘x’.
 ${}^x p_i^j$ Is probability of any output ‘i’ of any consequence model element ‘j’ feeding into the “source” consequence ‘x’ or the next consequence model element ‘x’.
 f_j Is the frequency at any consequence model element ‘j’, whose output ‘i’ is feeding into “source” consequence ‘x’ or the next consequence model element ‘x’.

It follows that the risk at the consequence model element equals to a sum of risks conveyed out through a consequence model element outputs and is equal to:

$$R_{MEj} = \sum_{i=1}^{i=5} Wr_i^j \quad \text{Equation 16}$$

Hence, loss at the model element ‘j’ equals to the risk at the consequence model element divided by frequency at the consequence model element:

$$L_{MEj} = \frac{R_{MEj}}{f_j} \quad \text{Equation 17}$$

Absolute importance of the consequence model element ‘j’, originating from Critical Event ‘h’ is equal to the maximum difference between outputs’ weights (risk conveyed through all outputs ‘i’ of a consequence model element ‘j’) to a “source” consequence ‘x’ or the next consequence model element ‘x’ and is expressed as:

$${}_{absolute} I_{MEj}^{ceh} = \max |Wr_i^j - Wr_{i-1}^j|_{i=2}^{i=5} \quad \text{Equation 18}$$

Where:

${}_{absolute} I_{MEj}^{ceh}$ Is an absolute importance of the consequence model element ‘j’.
 Wr_i^j Is weight of the output ‘i’ of a consequence model element ‘j’.
 Wr_{i-1}^j Is weight of the output ‘i-1’ of a consequence model element ‘j’.

$\max |Wr_i^j - Wr_{i-1}^j|_{i=2}^{i=5}$ Is maximum value of the difference in weight between all outputs ‘i’ of a consequence model element ‘j’.

Fractional importance of the consequence model element ‘ ω ’ ($1 \leq \omega \leq n$), originating from Critical Event ‘h’, relative to the whole consequence model structure is given by:

$$I_{MEj}^{ceh} = \frac{\text{absolute } I_{ME\omega}^{ceh}}{\sum_{j=1}^{j=n} \text{absolute } I_{MEj}^{ceh}} \quad \text{Equation 19}$$

Where:

$\text{absolute } I_{ME\omega}^{ceh}$ Is an absolute importance of the consequence model element ‘ ω ’, originating from Critical Event ‘h’.

$\sum_{j=1}^{j=n} \text{absolute } I_{MEj}^{ceh}$ Is the sum of all absolute importance values of all the consequence model elements ‘j’, originating from Critical Event ‘h’.

Fractional importance of the consequence model element ‘ ω ’ ($1 \leq \omega \leq n$), to the “source” consequence ‘y’, originating from Critical Event ‘h’ is given by:

$$\text{scy } I_{ME\omega}^{ceh} = \frac{\text{scy } \text{absolute } I_{ME\omega}^{ceh}}{\sum_{j=1}^{j=n} \text{scy } \text{absolute } I_{MEj}^{ceh}} \quad \text{Equation 20}$$

Where:

$\text{scy } \text{absolute } I_{ME\omega}^{ceh}$ Is an absolute importance of the consequence model element ‘ ω ’, originating from Critical Event ‘h’ and on the path to the “source” consequence ‘y’.

$\sum_{j=1}^{j=n} \text{scy } \text{absolute } I_{MEj}^{ceh}$ Is the sum of all absolute importance values of all the consequence model elements ‘j’, originating from Critical Event ‘h’ and on the path to the “source” consequence ‘y’.

Fractional importance of the consequence model element ‘ ω ’ ($1 \leq \omega \leq n$), on the path to the “source” consequence ‘y’, to the virtual consequence ‘j’, at any level ‘l’, is relative to the fractional contribution of the “source” consequence ‘y’ ($1 \leq y \leq n$), originating from Critical Event ‘h’ to the virtual consequence ‘j’, and is given by:

$$\text{vj } I_{ME\omega}^{ceh} = \text{vj } A_{sy} \cdot \text{scy } I_{ME\omega}^{ceh} = \frac{\text{vj } R_{sy}^{ceh}}{\sum_{k=1}^{k=n} \sum_{i=1}^{i=n} \text{vj } R_{si}^{cek}} \cdot \frac{\text{scy } \text{absolute } I_{ME\omega}^{ceh}}{\sum_{j=1}^{j=n} \text{scy } \text{absolute } I_{MEj}^{ceh}} \quad \text{Equation 21}$$

Where:

$\text{scy } \text{absolute } I_{ME\omega}^{ceh}$ Is an absolute importance of the consequence model element ‘ ω ’, originating from Critical Event ‘h’ and on the path to the “source” consequence ‘y’.

$\sum_{j=1}^{j=n} \text{scy } \text{absolute } I_{MEj}^{ceh}$ Is the sum of all absolute importance values of all the consequence model elements ‘j’, originating from Critical Event ‘h’ and on the path to the “source” consequence ‘y’.

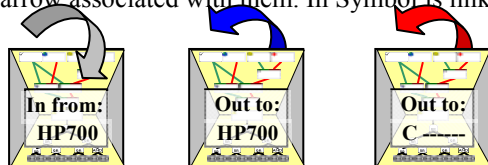
$\text{vj } R_{sy}^{ceh}$ Is the risk of the “source” consequence ‘y’ on whose path the consequence model element ‘ ω ’ is.

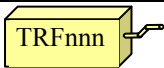
R_{vj}^l Is the risk of the virtual consequence ‘j’ at any Layer ‘l’ analysed.

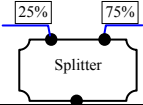
APPENDIX B: SPECIFICATION FOR CAUSE-CONSEQUENCE MODELS INTEGRATION ENVIRONMENT

Object Type/Class	
Critical Event Model super object (real consequences and base events of the model)	
Object Attributes	Each of the Cause-Consequence models within ISAE is presented through two distinguished sets of records: 1. A record set providing basic information about all the consequences arising from the model (consequence name and reference number) and, 2. Basic information about all the base events c from the model (consequence name and reference number). Visual appearance is provided below. Real Consequences cannot receive any frequencies from outside models. Real Consequences can only fed into base events of other models, <i>intermittent operators</i> or into high level/virtual consequences. Multi coloured circles present linking points: 1. Real consequences linked to virtual consequences have red circles associated with them; 2. Real consequences linked to <i>intermittent operator</i> have green circles associated with them; 3. Real consequences linked to base events of other models have blue circles associated with them, and 4. Critical events linked to base events of other models have orange circles associated with them 5. Real consequences that are disabled (not to be taken into account for calculations of total risk, but still calculated for individual models risk) are to be notified by grey circles. Real consequences can be disabled manually, through a control switch or if the critical event has been linked as the feeder to the base event of some other model. Base events can be linked to other models only as recipients of frequencies coming out of consequences or critical events calculated within external models or <i>intermittent operator</i> linked to consequences. Base events can be fed by real consequences or critical events of other models. Base events related linking points are presented by collared circles as follows: 1. Base events fed by real consequences/critical events of other models are presented by blue circles; 2. Base events that are independent from other models are presented by grey circles; 3. In case of common base events (same base events recurring throughout several different models, but not necessarily with the same frequency) these are notified by green circles; 4. Base events determining the probability of the barrier failure are notified by black circles. Values for these base events are expressed as probabilities only.
Object Referencing	References of Cause-Consequence models are same as references of the Critical Events the models are built around. References of real consequences, critical events and base events are the same as the references within the model.
Object Representation	
Data referencing	1. Data transferred from a real consequence to the base event is referenced as follows: FROM “consequence reference” TO “base event reference”.

Object Type/Class	
Critical Event Model super object (real consequences and base events of the model)	
	2. Data transferred from a critical event to the base event is referenced as follows: FROM “critical event reference” TO “base event reference”. 3. Data transferred from the real consequence to the virtual consequence is referenced as follows: FROM “consequence reference” TO “virtual consequence reference” 4. Data transferred from the real consequence to the <i>intermittent operator</i> is referenced as follows: FROM “consequence reference” TO “<i>intermittent operator</i> reference” 5. Data transferred from a critical event to the base event is referenced as follows: FROM “critical event reference” TO “base event reference”. 6. Data transferred from the critical event to the <i>intermittent operator</i> is referenced as follows: FROM “critical event reference” TO “<i>intermittent operator</i> reference”
Object values and default conditions/data	Default values for base events are values provided originally within the model. If the base event is linked with other model’s consequence or critical event then the value of the base event is the frequency of the consequence/critical event calculated by the other model. A default value of virtual consequences is null for all the loss categories risks of the consequence. Real consequences feeding the virtual consequence are passing risks calculated by individual models for all the loss categories to the virtual consequence. Value of risk for each loss category within the virtual consequence is calculated as a sum of all the risks passed to the virtual consequence from all the real consequences feeding the virtual consequence.
Combinational Rules	1. Only frequencies are passed from real consequences to base events; 2. Linked base events can not be in AND relationship with other base events with frequencies used as units within the model structure. If this is the case then a warning message must be displayed. It is possible that frequency feeding the base event can be translated into probability using the <i>TRANSFER FUNCTION</i> object; 3. Risk calculated for each loss category are passed from real consequences to virtual consequences; 4. Aggregated risks are passed from a virtual consequence to virtual consequence; 5. It is ensured that no closed loops are formed within the integrated model; 6. Frequencies are passed from critical events to base events if the base event is determining the frequency of the critical event; 7. If the base events defined by the other model are within the fault trees that determine the probability of the barrier failure, it must be ensured that the total outcome of such a fault tree is expressed as a probability 8. All the rules applicable within the existing ISAE should still apply.
Working Environment of the object	Model Integration Environment

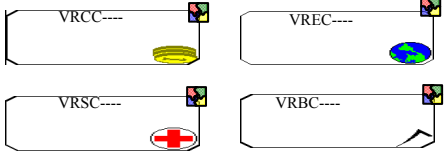
Object Type/Class	
Inter-model IN and OUT linking objects/symbols	
Object Attributes	These two objects are used for linking between two models during the modelling, from within one work sheet to another. “In From: - - - “ object feeds into the selected base event. “Output to: - - - “ object feeds into selected base event of another model, selected virtual consequence or <i>intermittent operator</i>. These two objects are in correspondence with links established through Critical Event Model super object, i.e. all the links between models created within the Model Integration Environment are automatically mimicked by IN and OUT symbols, automatically created within the corresponding models worksheets. Inverse applies as well, i.e. links defined through the models worksheets, using IN and OUT symbols are mimicked by the Model Integration Environment. Visual appearance is provided below.
Object Referencing	Objects are referenced as follows: 1. Out to virtual consequence symbol: “Out to: <i>virtual consequence reference</i>”; 2. Out to base event symbol: “Out to: <i>base event/critical event (other model) reference</i>”; 3. In from symbol: “In from: <i>consequence/critical event (other model) reference</i>” or “In from: <i>intermittent operator reference</i>”.
Object Representation	OUT symbols: Real consequences linked to virtual consequences have red arrow associated with them and real consequences or critical events linked to base events of other models have blue arrow associated with them. Real consequences are linked to OUT symbol by blue or red line. IN symbols: IN symbol have grey arrow associated with them. In Symbol is linked to base event by grey line. 
Data referencing	Data transferred from a real consequence to the base event is referenced in the following way: FROM “consequence reference/critical event” TO “base event reference”. Data transferred from the real consequence to the virtual consequence is referenced as: FROM “consequence reference” to “virtual consequence reference”
Object values	Objects take values as follows: 1. Out to virtual consequence symbol: risks calculated by individual models for all the loss categories; 2. Out to base event symbol: the frequency of the consequence calculated by the model; 3. In from symbol: risks calculated by individual models for all the loss categories or the frequency of the consequence (link from) calculated by the other model; 4. Default values for base events are values provided originally within the model. If the base event is linked with other model’s consequence than the value of the base event; 5. Default value of virtual consequences is null for all the loss categories risks of the consequence. Value of risk for each loss category within the virtual consequence is calculated as a sum of all the risks passed to the virtual consequence from all the real consequences feeding the virtual consequence.
Combinational Rules	1. IN symbol can fed in Base Event only; 2. Base events can be linked to other models only as recipients of frequencies coming out of consequences/critical events calculated within external models; 3. Real consequences/critical events cannot receive any direct input from outside models. Real consequences can only fed into base events of other models or into high level/virtual consequences; 4. Critical event can only fed into base events of other models. 5. If the base events defined by the other model are within the fault trees that determine the probability of the barrier, it must be ensured that the total outcome of such a fault tree is expressed as a probability (self check must operate on the structure instantaneously).
Object controls/data fields	Fields providing the information about the values passed through the link. In case of an IN symbol, i.e. link from a real consequence to the base event, frequency passed is displayed within the symbol’s dialog box. In case of an OUT symbol two possibilities exist: 1. If the link is between the real consequence/critical event and the base event information displayed within the symbol’s dialog box should be the frequency passed through the link; 2. If the link is between the two consequences (any consequences) the information passed

	through the link shall be risk calculated for all the existing risk categories.
Working Environment of the object	Individual models worksheets
Object Type/Class	
Transfer function <i>intermittent operator</i>	
Object Attributes	This object can have multiple inputs and outputs. Inputs are processed according to the “transfer function” defined within the object to yield outputs. For the transfer function it is possible to define inputs and outputs as the parameters of the “transfer function”. Inputs may come from real consequences or high level/virtual consequences only or critical events. Two types of inputs may exist: 1. If inputs are risks passed through, from consequences, the object must support distinction between different categories of risks. Therefore it is possible to define each of the risk categories as a separate parameter as well as to lump them all together if needed. In this case outputs must be risks as well; 2. If inputs are frequencies/probabilities passed from the consequences/critical events to the object the object shall support a simple allocation of the input to the parameter. In this case outputs may be either frequencies or risks depending on the nature of the transfer function. Four types of parameters may be used: 1. Parameters used/defined to identify inputs; 2. Parameters used/defined to identify outputs; 3. Parameters defined to establish/build the transform function; 4. Parameters already existing within the database and used to establish/build the transform function. Immediate calculation of the “transform function” shall be available allowing for the modeller to check the function and results instantly.
Object Referencing	Object is referenced as TRFnnn, where TRF is a prefix and nnn is three digit identification.
Object Representation	
Data referencing	1. Each of the inputs is referenced separately as an input to the object. 2. Each of the outputs is referenced separately as an output of the object. 3. The transfer function is referenced to the object. 4. All the additional information such as “rationale, justification, etc. are referenced to the object. 5. All the parameters defined are referenced individually, or if parameters already defined elsewhere are to be used then reference to these parameters relative to the object must be established.
Object values	Calculated or defaulted values.
Default conditions/data	Transfer function is “null”, i.e. inputs to the object are not linked to the outputs of the object (outputs of the object are set to zero).
Combinational Rules	1. All the inputs into the object must be of the same units, either frequencies or risks; 2. Combination of inputs defined by the transfer function yields outputs defined by the transfer function; 3. If the output is to be linked to the base event then the unit of the output can be frequency or probability depending on the causal model structure the base event is positioned within; 4. If the output is to be linked to the consequence then the unit of the output must be the risk calculated for all the risk categories.
Working Environment of the object	Model Integration Environment

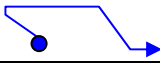
Object Type/Class	
Splitter <i>intermittent operator</i>	
Object Attributes	Two types of inputs may exist: 1. If inputs are risks passed through, from consequences, the object supports distinction between different categories of risks. Therefore it is possible to define each of the risk categories as a separate input as well as to lump them all together if needed. Split is either per individual risk category or for the total/lumped value. Outputs must be risks as well. 2. If inputs are frequencies/probabilities passed from the consequences to the object, the object supports a simple allocation of the input to the parameter. Outputs must be frequencies. Other attributes are same as for the splitter already existing within the worksheet environment.
Object Representation	
Working Environment of the object	Model Integration Environment

Object Type/Class	
Logical Gates (AND, OR) <i>intermittent operators</i>	
Object Attributes	The algorithm for calculations of gates is provided within the causal domain specification. Only links from real consequence or critical event to the base event can be linked to the gate. In case of an AND gate all the frequencies feeding the gate except for one, must be transferred into probabilities within the Transfer function object. Links from real consequence/virtual consequence to virtual consequence cannot be linked into gates.
Object Representation	
Combinational Rules	Only Links from real consequence/critical event to base events can be linked to the gate. No more than one frequency can fed the AND gate.
Object controls/linking and processing	Linking of inputs into the gate Linking of output from the gate Processing (same as described within the causal analysis tool specification)
Working Environment of the object	Model Integration Environment

Object Type/Class	
Supper Connectors <i>intermittent operators</i>	
Object Attributes	Unlimited number of inputs into this object and only one output. The output of this object is the sum of all the inputs.
Object Referencing	Same/similar as the super-connector within the existing individual models worksheets environment.
Object Representation	
Object values	The output of the object is the sum of all the inputs. All the inputs must be of the same type i.e. either frequencies, probabilities or risks. If inputs are frequencies/ probabilities the output is the sum of all the frequencies/ probabilities. If inputs are risks the output is the sum of all the inputs but aggregation must be done individually for each risk category. Consequently the output in this case will be in form of 13 values, one for each risk category.
Combinational Rules	All the inputs must be of the same type i.e. either frequencies or risks.
Working Environment of the object	Model Integration Environment

Object Type/Class	
Virtual Consequences	
Object Attributes	The value of these objects is calculated as the sum of risks for each risk category for all the feeders into the virtual consequence.
Object Representation	
Default conditions/data	Default value is null.
Working Environment of the object	Model Integration Environment

Object Type/Class	
Links from real/ virtual consequence to virtual consequence	
Object Attributes	Only risks calculated for each risk category shall be passed by the link.
Object Representation	
Combinational Rules	Link from the real/ virtual consequence to the virtual consequence or any of the intermittent operators
Working Environment of the object	Model Integration Environment

Object Type/Class	
Links from real consequence to base event	
Object Attributes	Only frequency calculated for the consequence shall be passed through the link.
Object Referencing	To be defined
Object Representation	
Data referencing	To be defined
Object values	Frequency calculated for the consequence
Combinational Rules	Links from the real consequence to the base event or any of the intermittent operators.
Working Environment of the object	Model Integration Environment

Object Type/Class	
Links from the critical event to the base event	
Object Attributes	Only frequency calculated for the critical event shall be passed through the link.
Object Representation	
Object values	Frequency calculated for the critical event
Combinational Rules	Links from the critical event to the base event or any of the intermittent operators.
Working Environment of the object	Model Integration Environment