A Bayesian Network Methodology for Railway Risk, Safety and Decision Support

A dissertation submitted to the
Fakultät Verkehrswissenschaften ''Friedrich List'' of
TECHNISCHE UNIVERSITÄT DRESDEN

for the degree of

Doktoringenieur (Dr.-Ing.)

Presented by

Qamar Mahboob (M.Sc, M.Sc.)
Born on 10 May 1978, Multan (Pakistan)

Submitted on 12.11. 2013
Defended on 14.02.2014

Supervisor:
Prof. Dr.-Ing. Jochen Trinckauf (TU Dresden), advisor and examiner

Doctoral commission:
Prof. Dr.-Ing. Günter Löffler (TU Dresden), Chairman
Prof. Dr.-Ing. Jochen Trinckauf (TU Dresden), advisor and examiner
Prof. Dr. sc. tech. (ETH) Daniel Straub (TU München), examiner
PD. Dr.-Ing. habil. Waltenegus Dargie (TU Dresden)
Prof. Dr. rer. nat. habil. Karl Nachtigall (TU Dresden)

A Bayesian Network Methodology for Railway Risk, Safety and Decision Support

by

Qamar Mahboob

To my wife Quratulain, daughter Sarah, parents and other family members and friends.

Thank you…

I will never believe that God plays dice with the universe.

Albert Einstein

ACKNOWLEDGEMENTS

I would like to thank all the people that influenced my trajectory through this end. I will take the risk to forget some of them, but I thank them all in advance.

The development of this dissertation could not have been possible without the unmatched support and guidance of Professor Jochen Trinckauf. I would like to thank him for his valuable supervision. He gave me the freedom to search my way and direction to find it.

Special thanks go to Professor Dr. Daniel Straub of Technische Universität München, who has been always my main source of motivation and inspiration in the field of risk, safety and reliability. He supported me, both professionally and personally and corrected my work at different stages. I also express my deep gratitude to him for acting as an examiner on this work.

I am grateful to many technical experts who have provided guidance and advice in order to improve the quality of this thesis. Especially, I would like to send many thanks to Dr. Daniela Manuela Hanea (Senior Safety and Asset Risk Management consultant at Det Norske Veritas and former associate professor at TU Delft) for time to time corrections and many valuable advises about how to improve the work. I also wish to thank PD. Dr.-Ing. habil. Waltenegus Dargie of TU Dresden for useful discussions related to prediction and estimation techniques.

I could not have finished this study, without the lunches, coffee breaks and much more in- and outside our work environment with current and former colleagues from TU Dresden and TU München. So, many thanks to all my colleagues for their support and the time I had during my PhD studies. Importantly, I am grateful to Christoph Hoefert, Christoph Klaus, Claudia Machner, Daria Bachurina, Eva Günther, Elena Kosukhina, Eric Schöne, Giulio Cottone, Jens Buder, Johannes Fischer, Lisa Herzler, Martin Sommer, Michael Kunze, Olga Spackova, Patty Papakosta, Simona Miraglia, Ulrich Maschek and Uwe Lehne.

Financial support for this study was provided by the Higher Education Commission of Pakistan, the Deutsche Akademischer Austausch Dienst (DAAD) Germany, the Technische Universität Dresden, CERSS Kompetenzzentrum Bahnsicherungstechnik Dresden and Pakistan Railways. This support is gratefully acknowledged.

STATEMENT OF ORIGINALITY

I declare that to the best of my knowledge the research work presented in this thesis is original except as acknowledged and cited in the text, and that the material has not been submitted, either in whole or part, for another degree at any university elsewhere. This thesis is prepared on my own.

I accept the regulations of the Fakultät Verkehrswissenschaften ‘’Friedrich List’’ of Technische Universität Dresden that are applicable to a German PhD degree.

Signed:----------Qamar Mahboob

Date: 19.02.2014, Dresden

ABSTRACT

For railways, risk analysis is carried out to identify hazardous situations and their consequences. Until recently, classical methods such as Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) were applied in modelling the linear and logically deterministic aspects of railway risks, safety and reliability. However, it has been proven that modern railway systems are rather complex, involving multi-dependencies between system variables and uncertainties about these dependencies. For train derailment accidents, for instance, high train speed is a common cause of failure; slip and failure of brake applications are disjoint events; failure dependency exists between the train protection and warning system and driver errors; driver errors are time dependent and there is functional uncertainty in derailment conditions. Failing to incorporate these aspects of a complex system leads to wrong estimations of the risks and safety, and, consequently, to wrong management decisions. Furthermore, a complex railway system integrates various technologies and is operated in an environment where the behaviour and failure modes of the system are difficult to model using probabilistic techniques. Modelling and quantification of the railway risk and safety problems that involve dependencies and uncertainties such as mentioned above are complex tasks.

Importance measures are useful in the ranking of components, which are significant with respect to the risk, safety and reliability of a railway system. The computation of importance measures using FTA has limitation for complex railways. ALARP (As Low as Reasonably Possible) risk acceptance criteria are widely accepted as *''best practice''* in the railways. According to the ALARP approach, a tolerable region exists between the regions of intolerable and negligible risks. In the tolerable region, risk is undertaken only if a benefit is desired. In this case, one needs to have additional criteria to identify the socio-economic benefits of adopting a safety measure for railway facilities. The Life Quality Index (LQI) is a rational way of establishing a relation between the financial resources utilized to improve the safety of an engineering system and the potential fatalities that can be avoided by safety improvement. This thesis shows the application of the LQI approach to quantifying the social benefits of a number of safety management plans for a railway facility.

We apply Bayesian Networks and influence diagrams, which are extensions of Bayesian Networks, to model and assess the life safety risks associated with railways. Bayesian Net-

works are directed acyclic probabilistic graphical models that handle the joint distribution of random variables in a compact and flexible way. In influence diagrams, problems of probabilistic inference and decision making – based on utility functions – can be combined and optimized, especially, for systems with many dependencies and uncertainties. The optimal decision, which maximizes the total benefits to society, is obtained.

In this thesis, the application of Bayesian Networks to the railway industry is investigated for the purpose of improving modelling and the analysis of risk, safety and reliability in railways. One example application and two real world applications are presented to show the usefulness and suitability of the Bayesian Networks for the quantitative risk assessment and risk-based decision support in reference to railways.

ZUSAMMENFASSUNG

In Bahnsystemen werden Risikoanalysen durchgeführt, um gefährliche Situationen und deren Konsequenzen zu identifizieren. Bisher wurden herkömmliche Methoden wie Fehlerbaumanalyse (FTA, Fault Tree Analysis) und Ereignisbaumanalyse (ETA, Event Tree Analysis) angewendet, um lineare und logisch-deterministische Aspekte der Risiken im Bahnsystem zu modellieren. Es hat sich jedoch gezeigt, dass moderne Bahnsysteme zunehmend komplex sind und mehrfache Abhängigkeiten zwischen den Systemparametern sowie Ungewissheiten über diese Abhängigkeiten beinhalten. Beispiele aus der Modellierung und Risikobewertung von Entgleisungsunfällen sind: hohe Zuggeschwindigkeit als Fehler mit gemeinsamer Ursache („Common-Cause-Failure"); Fehler beim Bremsvorgang und Gleiten als unabhängige Ereignisse; Abhängigkeiten zwischen Zugsicherungssystemen und Fehlern des Triebfahrzeugführers; zeitabhängige Fehler des Triebfahrzeugführers; funktionale Ungewissheiten über die Entgleisungsbedingungen.

Eine Vernachlässigung dieser Aspekte eines komplexen Systems führt zu falschen Schätzungen des Risikos und der Sicherheit und schließlich zu falschen Management-Entscheidungen. Weiterhin umfassen Bahnsysteme verschiedenartige Technologien und werden in Umgebungsbedingungen betrieben, in denen das Verhalten und Fehlerarten des Systems mit wahrscheinlichkeitstheoretischen Ansätzen schwer modellierbar sind. Die Modellierung und Quantifizierung von Risiken und Sicherheitsproblemen mit den oben erwähnten Abhängigkeiten und Ungewissheiten stellen komplexe Aufgaben dar.

Importanzmaße sind nützlich bei der Aufstellung einer Rangfolge der für Risiko, Sicherheit und Zuverlässigkeit des Bahnsystems bedeutenden Komponenten. Die Berechnung der Importanzmaße mittels Fehlerbaumanalyse stößt jedoch bei komplexen Bahnsystemen an ihre Grenzen.

Das Risikoakzeptanzkriterium ALARP (As Low As Reasonably Possible) findet als „best Practice" in der Bahnindustrie breite Anerkennung. Nach diesem Ansatz existiert zwischen dem Bereich nicht tolerierbarer und dem Bereich vernachlässigbarer Risiken ein tolerierbarer Bereich. In diesem Bereich wird Risiken nur begegnet, wenn daraus ein Nutzen zu erwarten ist. Hierbei werden zusätzliche Kriterien benötigt, um den sozioökonomischen Nutzen von Sicherheitsmaßnahmen zu ermitteln. Der Life-Quality-Index (LQI) ist ein

vernünftiger Weg, um ein Verhältnis zwischen den finanziellen Ressourcen zur Verbesserung der Sicherheit eines technischen Systems einerseits und den durch die Sicherheitsmaßnahme potenziell vermeidbaren Opfern andererseits herzustellen. Die Arbeit zeigt die Anwendung des LQI-Ansatzes auf das Bahnsystem, wobei der sozioökonomische Nutzen verschiedener Sicherheitsmanagementpläne für Bahnanlagen quantifiziert wird.

Schließlich werden Bayes'sche Netze und Einflussdiagramme angewendet, um die mit Bahnsystemen verbundenen Lebensrisiken zu modellieren und einzuschätzen. Bayes'sche Netze sind gerichtete azyklische wahrscheinlichkeitstheoretische Graphen, die Verteilungen von Zufallsgrößen in kompakter und flexibler Weise behandeln. Durch Einflussdiagramme können die Probleme der wahrscheinlichkeitstheoretischen Schlussfolgerung und der Entscheidungsfindung – basierend auf Nutzenfunktionen – kombiniert und optimiert werden, insbesondere für Probleme mit vielen Abhängigkeiten und Ungewissheiten. Man erhält die optimale Entscheidung, die den Gesamtnutzen für die Gesellschaft maximiert.

In der vorliegenden Arbeit wird die Anwendung Bayes'scher Netze auf die Bahnindustrie zum Zwecke der verbesserten Modellierung und Analyse von Risiko, Sicherheit und Zuverlässigkeit untersucht. Dabei erfolgen eine Beispielanwendung und zwei reale Anwendungen, mit denen der Nutzen und die Eignung Bayes'scher Netze zur quantitativen Risikoanalyse und risikobasierten Entscheidungsfindung für Bahnsysteme gezeigt werden.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS ..... **IV**

ABSTRACT ..... **VI**

ZUSAMMENFASSUNG ..... **VIII**

LIST OF FIGURES ..... **XIV**

LIST OF TABLES ..... **XVI**

CHAPTER 1: Introduction **1**

1.1 Need to model and quantify the causes and consequences of hazards on railways 1

1.2 State-of-the art techniques in the railway 2

1.3 Goals and scope of work 4

1.4 Existing work 6

1.5 Outline of the thesis 7

CHAPTER 2: Methods for safety and risk analysis **10**

2.1 Introduction 10

2.1.1 Simplified risk analysis 12

2.1.2 Standard risk analysis 12

2.1.3 Model-based risk analysis 12

2.2 Risk Matrix 14

2.2.1 Determine the possible consequences 14

2.2.2 Likelihood of occurrence 15

2.2.3 Risk scoring matrix 15

2.3 Failure Modes & Effect Analysis – FMEA 16

2.3.1 Example application of FMEA 17

2.4 Fault Tree Analysis – FTA 19

2.5 Reliability Block Diagram – RBD 22

2.6 Event Tree Analysis – ETA 24

2.7 Safety Risk Model – SRM 25

2.8 Markov Model – MM 27
2.9 Quantification of expected values 31
2.9.1 Bayesian Analysis – BA 35
2.9.2 Hazard Function – HF 39
2.9.3 Monte Carlo (MC) Simulation 42
2.10 Summary 46

CHAPTER 3: Introduction to Bayesian Networks 48
3.1 Terminology in Bayesian Networks 48
3.2 Construction of Bayesian Networks 49
3.3 Conditional independence in Bayesian Networks 51
3.4 Joint probability distribution in Bayesian Networks 52
3.5 Probabilistic Inference in Bayesian Networks 53
3.6 Probabilistic inference by enumeration 54
3.7 Probabilistic inference by variable elimination 55
3.8 Approximate inference for Bayesian Networks 57
3.9 Dynamic Bayesian Networks 58
3.10 Influence diagrams (IDs) 60

CHAPTER 4: Risk acceptance criteria and safety targets 62
4.1 Introduction 62
4.2 ALARP (As Low As Reasonably Possible) criteria 62
4.3 MEM (Minimum Endogenous Mortality) criterion 63
4.4 MGS (Mindestens Gleiche Sicherheit) criteria 64
4.5 Safety Integrity Levels (SILs) 65
4.6 Importance Measures (IMs) 66
4.7 Life Quality Index (LQI) 68
4.8 Summary 72

CHAPTER 5: Application of Bayesian Networks to complex railways: A study on derailment accidents 73
5.1 Introduction 73
5.2 Fault Tree Analysis for train derailment due to SPAD 74

5.2.1 Computation of importance measures using FTA 75
5.3 Event Tree Analysis (ETA) 78
5.4 Mapping Fault Tree and Event Tree based risk model to Bayesian Networks 79
5.4.1 Computation of importance measures using Bayesian Networks 81
5.5 Risk quantification 82
5.6 Advanced aspects of example application 83
5.6.1 Advanced aspect 1: Common cause failures 83
5.6.2 Advanced aspect 2: Disjoint events 84
5.6.3 Advanced aspect 3: Multistate system and components 84
5.6.4 Advanced aspect 4: Failure dependency 85
5.6.5 Advanced aspect 5: Time dependencies 85
5.6.6 Advanced aspect 6: Functional uncertainty and factual knowledge 85
5.6.7 Advanced aspect 7: Uncertainty in expert knowledge 86
5.6.8 Advanced aspect 8: Simplifications and dependencies in Event Tree Analysis 86
5.7 Implementation of the advanced aspects of the train derailment model using Bayesian Networks. 88
5.8 Results and discussions 92
5.9 Summary 93

CHAPTER 6: Bayesian Networks for risk-informed safety requirements for platform screen doors in railways 94

6.1 Introduction 94
6.2 Components of the risk-informed safety requirement process for Platform Screen Door system in a mega city 97
6.2.1 Define objective and methodology 97
6.2.2 Familiarization of system and information gathering 97
6.2.3 Hazard identification and hazard classification 97
6.2.4 Hazard scenario analysis 98
6.2.5 Probability of occurrence and failure data 99
6.2.6 Quantification of the risks 105
6.2.6.1. Tolerable risks 105
6.2.6.2. Risk exposure 105
6.2.6.3. Risk assessment 106
6.3 Summary 107

CHAPTER 7: Influence diagrams based decision support for railway level crossings 108

7.1 Introduction 108

7.2 Level crossing accidents in railways 109

7.3 A case study of railway level crossing 110

7.4 Characteristics of the railway level crossing under investigation 111

7.5 Life quality index applied to railway level crossing risk problem 115

7.6 Summary 119

CHAPTER 8: Conclusions and outlook 120

8.1 Summary and important contributions 120

8.2 Originality of the work 122

8.3 Outlook 122

BIBLIOGRAPHY 124

APPENDIX 1 131

LIST OF FIGURES

Figure 2.1: Interaction of RAMS components, after (Sapoznikov, et al., 2009) 11

Figure 2.2: An example of a cause and consequence diagram..... 13

Figure 2.3: Components of the ballasted track..... 17

Figure 2.4: A Fault Tree for Train derailment (Mahboob, et al., 2012(d)). 20

Figure 2.5: Reliability block diagram for train derailment due to signal passed at danger. 23

Figure 2.6: A sample Event Tree analysis for Top Event '' Wrong opening of platform screen doors when train is departing'' (Mahboob, et al., 2013)..... 24

Figure 2.7: Safety risk model or Bow-Tie model ROSA (Puettner & Geisler, 2008). 27

Figure 2.8: A Markov Model for system safety and availability, after (Anders, 2008)..... 29

Figure 2.9: Failure probability of (non-repairable) railway facility as a function of time. 31

Figure 2.10: Comparison of the prior and posterior knowledge for the discrete case of Bayes' theorem. 37

Figure 2.11: Prior, likelihood and posterior PDFs of soil strength for railway track..... 39

Figure 2.12: Hazard and reliability functions based on Weibull failure distribution..... 41

Figure 2.13: Hazard function for the 2-out- of-3 (independent and identically distributed) non-repairable system. 42

Figure 2.14: Illustration of the capacity and demand problem from the field of structural reliability. 44

Figure 2.15: Normally distributed random variables corresponding to capacity (R) and demand (S). 46

Figure 3.1: A sample Bayesian Network 49

Figure 3.2: (Conditional) Probability tables for $\boldsymbol{X1, \ldots, X4}$. 50

Figure 3.3: Conditional probability table for $\boldsymbol{X5}$. 51

Figure 3.4: A graphical representation of d-separation properties of Bayesian Networks connections. 52
Figure 3.5: Bayesian Networks framework obtained during probabilistic inference by variable elimination. 57
Figure 3.6: Schematic representations of a Dynamic Bayesian Network model (DBN). 59
Figure 3.7: A concise representation of dynamic Bayesian Network. 59
Figure 3.8: A sample influence diagram for prior analysis. 60
Figure 4.1: An ALARP based individual and collective risk acceptance criteria. 63
Figure 4.2: The Minimum Endogenous Mortality based criteria for risk acceptance. 64
Figure 4.3: A definition of safety integrity levels (SILs). 65
Figure 4.4: Illustration of the Life Quality Index (LQI) principle (Nishijima, 2012). 69
Figure 5.1: A safety risk model for train derailment. 76
Figure 5.2: Mapping of a Fault Tree and Event Tree based model to Bayesian Network. 79
Figure 5.3: Bayesian Networks model equivalent to the FT & ET based model. 81
Figure 5.4: Fault Tree Analysis of Train Derailment after considering three advanced aspects. 88
Figure 5.5: Bayesian Networks based safety risk model including advanced aspects of the FT & ET based safety risk model. 91
Figure 6.1: A platform screen door system installed at the Sao Paulo, Brazil 95
Figure 6.2: Components of the risk-informed safety requirement process for PSD systems (Mahboob, et al., 2013) 96
Figure 6.3: Bayesian Networks based consequence analysis for risk reduction factor. 99
Figure 7.1: ALARP individual risk acceptance criteria for a level crossing problem 109
Figure 7.2: Influence diagram for decision optimization of a level crossing facility. 111

LIST OF TABLES

Table 2.1: An example of ranking the possible consequences. 15

Table 2.2: Likelihood of occurrence. 15

Table 2.3: Risk calculation by using scoring matrix. 16

Table 2.4: Example of FMEA – damage to rail sleeper. 18

Table 2.5: Discrete case of posterior probability. 37

Table 4.1: Selected importance measures and their brief definitions. 67

Table 5.1: Basic events for the causes of train derailment and their fixed unavailability (FUV) and failure frequency (FF). 75

Table 5.2: IMs computed from Fault Tree Analysis. 77

Table 5.3: Safety integrity levels (SILs) level for different consequences of train derailment. ... 78

Table 5.4: Numerical mapping of AND gate for speed & alignment (SA) in FT to equivalent probability table in Bayesian Networks. 80

Table 5.5: Risk reduction factors computed from the models. 83

Table 5.6: Basic events for modelling multistate event for train derailment model. 84

Table 5.7: XOR logic for Conditions for derailment. 85

Table 5.8: Conditional probability table for node slip. 89

Table 5.9: Conditional probability table for node situations. 89

Table 5.10: Conditional probability table for TPWS fails and driver errors. 90

Table 5.11: Values of importance measure from Bayesian Networks after advanced aspects. 91

Table 7.1: Traffic conditions at level crossing. 113

Table 7.2: Individual risks from different types of level crossings. 114

Table 7.3: Costs (in €) to calculate societal capacity to commit resource using LQI. 115

Table 7.4: Societal capacity to commit resources towards different level crossings. 117

Table 7.5: LQI based costs for different LCs when fatalities are observed. 117

Table 7.6: Expected utilities (€ per year) of different safety measures for LC. 118

CHAPTER 1: INTRODUCTION

1.1 Need to model and quantify the causes and consequences of hazards on railways

Rail transportation is an important mode of transport throughout the world. Each day, it transports millions of passengers and goods from one point to another. For instance, Germany has the highest number of train-kilometres in Europe (1,063 million of train-kilometres in 2011) and the railway system serves as the backbone of the country's land transportation. The German railway has the highest passenger volume in the EU (85,035 million of passenger-kilometres in 2011) and has had increasing trends over the past three years. Probably, one of the reasons for the high and increasing passenger-volume on German (and many other) world railways is that the fatality risks for railway passengers are among the lowest in land transportation. For instance, one most recently available study in the EU confirms that railway passengers have lower travelling risks (0.156 fatalities per billion passenger-kilometres) in comparison to other means of land transportation such as buses (0.433 fatalities per billion passenger-kilometres), cars (4.450 fatalities per billion passenger-kilometres) and motor-cycles (52.593 fatalities per billion passenger-kilometres) (EU, 2012). Although the safety performance of railways in EU member states is high, serious accidents continue to occur. For example, a fatal train accident occurred on 24 July, 2013 near to Santiago de Compostela due to high train speed on a curve causing 80 fatalities and dozens of serious injuries (Spiegel, 2013). Each year, a number of lives are lost due to railway accidents. A recent report published by the European Railway Agency (ERA) indicates that every year there are approximately 2,400 accidents in EU leading to approximately 1,200 fatalities. Additionally, there are more than 1,000 serious injuries as a result of these accidents (ERA, 2013). The economic burden of the fatalities and serious injuries was valued at more than € 2.5 billion in 2011.

The safety and reliability of railway operation and their passengers depend on the reliability and safety of railway personnel, sub-systems and different technical components. A number of accidents will occur if the personnel, sub-systems and or components fail to act and work safely. For instance, a study grouped railways accidents into three categories; *rolling stock* (47%), *rail and track* (39%) and *insufficient information* (14%) (Holmgren, 2005). The same study further identified that the *rail and track* related accidents are mainly caused by maintenance (30%), railway operation (30%), sabotage (27%) and unknown causes (13%). Poor maintenance, for instance, mainly leads to mechanical failures. Some mechanical failures, such as wheel defects, traction motor defects, and control system problems, were reported to be the main causes for delays in commuter service in North American cities (Nelson & O'Neil, 2000). In addition, the railway systems are subject to a variety of natural hazards. Through improved risk, safety and reliability modelling techniques, it is possible to improve the quantification and evaluation of the failure causes and their consequences for railways.

1.2 State-of-the art techniques in the railway

A number of technical systems and solutions have been introduced to reduce failures and for safer operation of railways (Maschek, 2012). Methods exist to analyse the failures and their consequences on the technical systems and solutions (Ericson, 2005). For example, Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) are common techniques used for logical representation of a railway system for the purpose of risk and reliability analysis (Chen, et al., 2007; Braband, et al., 2006; Dhillon, 2007; Bearfield & Marsh, 2005). FTA is based on top-down logic, starting from the hazard, also called the Top Event (TE), and looking downwards at all possible combinations of causes of that hazard. ETA models the scenarios following the hazard and leading to different consequences such as property losses and fatalities. Very often, FTA and ETA are combined in one model, also called a bow-tie, which analyses the causes and the consequences of an accident (Khakzad, et al., 2013). In the railway industry, a combination of the two methods has been used to compute Individual Risk of Fatality (IRF) and safety integrity requirements for a technical system (Braband, et al., 2006). In general, both FTA and ETA are based on assumptions which simplify the compu-

tations, such as independent failures or logically deterministic combinations of causes. It has been proven that the railway system is rather complex, involving multi-dependencies between system variables and uncertainties about these dependencies. For example, high train speed is a common cause of failure; slip and failure of brake applications are disjoint events; failure dependency exists between the train protection and warning system and driver errors; driver errors are time dependent and there is functional uncertainty for derailment conditions. Failing to incorporate these complex aspects leads to wrong estimations of the risks and reliability, and, consequently, to wrong management decisions. Modelling and quantification of the railway risk and reliability problems that involve dependencies and uncertainties as mentioned above are complex tasks and require the application of an appropriate tool. FTA has limitations in modelling complex systems (Khakzad, et al., 2011; Xing & Amari, 2008). In most cases, the FTA structure increases exponentially, becoming non-intuitive and computationally demanding with an increase in, for example, common cause failures, disjoint events and multistate events (Mahboob, et al., 2012(c)). These limitations make the application of classical methods for the analysis of railway systems difficult.

Importance measures (IMs) can be used to identify and then rank the system components with respect to their significance towards risk and reliability. IMs can help system designers in identifying the components that should be improved, assist maintenance engineers to improve maintenance plans for the more critical components and facilitate decision making on the utilization of engineering budgets for human safety. A number of IMs exist that can be used for different identifications and rankings (Birnbaum, 1969; Rausand & Hoyland, 2004; Borgonovo & Apostolakis, 2001). For instance, Risk Achievement Worth (RAW) identifies the increase in the system risks if a particular component failure in the system has occurred. The Fussell-Vesely (FV) value gives the fractional contribution of a component failure towards the system failure. An increase in the occurrence probability of the component failure will lead to an increase in the FV value. For the application of IMs to different industries we refer to (Borgonovo, et al., 2003; Prescott & Andrews, 2010; Mahboob, et al., 2012(b)).

ALARP is widely accepted as ‘’best practice’’ into the railway industry (Braband, et al., 2006; Beugin, et al., 2007). ALARP provides several variations in between the two extremes. In other words, a tolerable region exists between the regions of intolerable and negligible risks. If the risks fall in the intolerable region then one should adopt safety measures

– regardless of cost – to bring the risks into the tolerable region or even below. In the tolerable region, risk reduction is desirable and is undertaken only if some benefit is obtained. The risk must be made as low as reasonably practicable in the tolerable region (Melchers, 2001). MEM (Minimum Endogenous Mortality) and MGS (Mindestens Gleiche Sicherheit) are also well applied risk acceptance criteria in the field of railways, see Chapter 4 for their brief introduction.

In many cases the problem of risk acceptance turns into an economic decision problem when the risks are in the so-called ALARP region and the objective is to further reduce the risks. In this situation, socio-economic considerations, such as benefit-cost analysis (BCA) have been utilized for railway risk management. In BCA, the profitability of a safety technology is calculated by quantifying the willingness-to-pay (WTP) (from the society point of view). WTP is the amount that people are willing to pay to save a human life. The BCA and the WTP approaches are well applied and usually accepted methods for valuing the prevention of fatalities (Evans, 2013; TD, 2000; Aoun, et al., 2012; RSSB, 2006; Evans, 2005). Of course, one can disregard BCA or WTP in the adoption of safety technology if the aim is to prevent and mitigate train collisions and derailments. The usual reason for the disregard is that a higher safety technology is needed than would be calculated by BCA. However, some areas of safety improvement such as upgrades or replacements of level crossings (LCs) are good subjects for BCA (Evans, 2013). The BCA takes into account the same parameters for the comparison of profitability of different safety technologies. Identification of such parameters for different socio-economic and geographical conditions and the assignment of monetary values (to benefits and costs) of the identified parameters always have complications. The BCA and WTP approaches become difficult to use if the parameters of the decision problem are not completely known.

1.3 Goals and scope of work

The goal of this research work is to investigate the application of Bayesian Networks as a decision support framework for railway risk and safety. This thesis explores various important aspects of the modelling and analysis of railway risks and how an improvement can be achieved in the risk-based decision making process. The work mainly focuses on the de-

velopment of a framework that can handle complexities and uncertainties in modern railways. It investigates how the economic considerations can be incorporated within the models so that the decision making on railway engineering budgets can further be facilitated. Visualization of the framework (in understanding the system variables, decision alternatives and risk acceptance criteria) is often required to facilitate the decision making process; therefore, compact and concise visualization of the model is necessary to provide a decision aid for the decision maker.

In view of the above, it has been determined that Bayesian Networks can provide a suitable tool to meet the modelling, analysis and decision support requirements above. Bayesian Networks are directed acyclic probabilistic graphical models that handle the joint distribution of random variables in a compact and flexible way. The following characteristics of Bayesian Networks make them suitable for railway risk, safety and decision support:

1) Bayesian Networks can handle multiple hazards and a number of dependencies and uncertainties among (the random variables of) different hazards and within a hazard. The dependencies can arise due to common cause, multistate and disjoint events in the hazard models.

2) Repetition of the random variables is not required for dependencies in Bayesian Networks. Thus, Bayesian Networks offer a concise and intuitive visualization of a framework which makes it useful for discussions among the designers, manufacturers, operators and decision makers who may not be expert in probabilistic risk assessment.

3) Bayesian Networks are able to update the hazard model in two ways. Top-down updating is obtained when the information propagates from the top, that is, from the hazard down to the basic causes of the hazards. In bottom-up updating, information propagates from the basic causes towards the hazard. For instance, by exploiting the use of the updating characteristics of the Bayesian Networks, one can account, at the same time, not only for the components that have failed, but also for those that are working.

4) Influence diagrams (IDs) are extensions of Bayesian Networks. Problems of probabilistic inference and decision making can be combined and optimized in IDs. They offers a decision tool for ranking alternatives based on expected utility.

In this thesis, we propose a Bayesian Network based methodology for performing railway risk and safety assessment. We show how the dependencies, uncertainties, expert knowledge and economics related aspects of a complex railway system can be tackled using Bayesian Networks for risk-based decision making.

1.4 Existing work

There are few applications of Bayesian Networks to railways. Importantly, these applications do not belong to the development of the IDs based decision framework for railway risks. (Marsh & Bearfield, 2007) use Bayesian Network for the representation of a parameterized FTA for SPAD[1]; (Oukhellou, et al., 2008) developed a Bayesian Network model for identifying and classifying rail defects based on sensor data; (Lu, et al., 2011) proposed a Bayesian Network approach to model the causal relationships among risk factors for subway systems; (Vatn & Svee, 2002) applied an influence diagram for decision making on the ultrasonic inspection of rails; (Flammini, et al., 2009) applied Bayesian Networks for quantitative security risk assessment and management for railway transportation infrastructures.

Risk models for railway accidents using IDs have not been studied extensively. No studies exist on how to model and analyse risks in complex railways – characterized by a number of advanced aspects, explained in Chapter 5 – using Bayesian Networks. The computation of the IMs for complex system's components using Bayesian Networks has not been discussed so far, especially, for railways. Therefore, the work in this thesis is novel with respect to the computation of IMs and the modelling and analysis of advanced aspects of risk models for complex railways using Bayesian Network and IDs based decision support for railway risks and safety cases. The LQI is a relatively new utility-based risk acceptance criterion and its application to the railway industry, to justify the investment in railway risks, is novel. How-

[1] SPAD (signal passed at danger) in railways occurs when a train passes a stop signal without permission to do so.

ever, the LQI is a well applied and accepted risk acceptance criterion from the field of structural safety. To the knowledge of the author, IDs based applied tools for railway risk management do not exist. However, some studies have suggested and developed such tools for fields other than railways (Hanea, 2009(a); Straub, 2005; Faber, et al., 2012; Bensi, et al., 2011).

1.5 Outline of the thesis

This thesis proposes a Bayesian Network methodology for risk assessment and decision support in reference to railways. The thesis is organized in 8 chapters. The motivation, state-of-the-art work and goals and scope of the research work are presented in the Introduction.

Chapter 2 provides an introduction to the methods for safety and risk analysis for railways. This chapter deals with the basic concepts and definitions of risk and safety. A review of the many existing methods and approaches, which are well applied to engineering risk problems, including railways engineering, is presented. A brief description is given for the simplest methods such as risk matrix, model based methods such as fault tree and numerical methods such as hazard function and Monte Carlo simulation. Each method is described with the help of a suitable example from the railways.

Chapter 3 reviews Bayesian Networks. Here, sufficient introduction to Bayesian Networks is provided so that methods and models presented in the following chapters can be better understood. It provides a brief introduction to terminology such as conditional independence, joint distribution and Markov blanket in a Bayesian Network. Construction of a Bayesian Network and probabilistic inference methods, such as inference by enumeration and variable elimination, are described with the help of examples. A brief introduction of IDs is presented.

Chapter 4 describes risk acceptance criteria and determination of safety targets in railways. The classical way of representing risks arising from a railway system is the individual risk which is expressed in terms of an annual fatality rate for a person exposed to the given situation at a given point in time. Individual risk acceptance criteria, based on the ALARP, MEM and MGS approaches, are explained. The LQI is also briefly explained in Chapter 4. The

LQI treats the risk acceptance criterion as an economic decision problem in an uncertain environment by establishing a relation between the resources utilized in improving the safety of a system and fatalities that can be avoided by the resources. It offers a rational way of finding acceptable decisions on engineering systems involving risks to human life.

The exact quantification of systematic errors (mainly caused by humans) is not possible; however, random failures can be quantified. The idea behind the safety integrity level (SIL) concept is to create a balance between the measures for preventing systematic errors and random failures.

This chapter explains the concept of IMs. The components with higher importance with respect to risk are treated carefully in the design, maintenance and operation of an engineering system. The definitions of selected IMs, which are used to identify and rank the important components in a system, are given here.

Chapter 5 provides an example application, which demonstrates the complexity of risk models in railways. The example of *train derailment* is used to show how Bayesian Networks can be used to model dependencies, uncertainties and expert knowledge for a railway risk problem. This chapter focuses on the modelling of advanced aspects of fault trees using Bayesian Networks. A fault tree and event tree based safety risk model is translated into a Bayesian Network, consequences of the railway hazard ‘’*train derailment*’’ are quantified and the IMs for the events leading to the hazard are computed.

Chapter 6 presents a real-world application of Bayesian Networks. Mega cities across the world will continue to grow during the 21st century. Urban rail transit systems (URTSs) in such mega cities are subject to different hazards, which can lead to life safety risks. Bayesian Networks are applied to quantify the risk-based safety integrity requirements for a PSD (Platform Screen Door) system in a typical mega city. The steps in the risk-informed safety requirement process are explained for the PSD system. A number of hazardous situations related to a PSD system, so-called hazardous situations, are identified. A preliminary cause and consequence analysis is carried out to scrutinize the most important hazardous situations. The consequences of these most relevant hazardous events are modelled for specific operational conditions. The identified consequences are quantified and then compared to

risk acceptance criteria for assessment. The risk-informed SIL requirements are determined for the PSD system.

Chapter 7 focuses on the justification of the investment in human safety in reference to a railway LC. We apply IDs to the assessment of life safety risks in a railway LC. Individual risk of fatality at a particular LC is determined for different safety technology solutions. The ALARP criteria in combination with the LQI are used to identify an optimal and socially acceptable safety solution for the LC. The LQI-based utilities are used in the IDs to optimize the decision problems.

Chapter 8 concludes the thesis by providing a summary, important contributions and suggesting future research work in this area.

CHAPTER 2: METHODS FOR SAFETY AND RISK ANALYSIS

2.1 Introduction

The railway system related standard EN 50126 (and CENELEC-Standard regarding functional safety 2006) introduces the RAMS (Reliability, Availability, Maintainability, and Safety) concept (CENELEC, 2012; Braband, et al., 2006). This standard provides RAMS specifications and requires the railway suppliers and operators to implement a RAMS management system and demonstrate particular safety standards. How the RAMS components influence each other is shown in Figure 2.1 (Sapoznikov, et al., 2009). The risk-oriented definitions of Reliability, Availability and Maintainability, based on the EN 50126, are given below.

RELIABILITY, $\boldsymbol{R(t)}$: The probability that an item can perform a required function under given conditions for a given time interval. Mathematically, it is written as

$$\boldsymbol{R(t) = 1 - F_T(t)}. \tag{2.1}$$

In the equation above, $F_T(t)$ is the distribution function for failure probability in time t.

MAINTAINABILITY, $\boldsymbol{M(t)}$: The probability that a given active maintenance action, for an item under given conditions of use, can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources.

AVAILABILITY, $\boldsymbol{A(t)}$: The ability of a product to be in a state to perform a required function under given conditions at a given instant of time, or over a given time interval, assuming that the required external sources of help are provided. The availability of a non-

repairable system is equivalent to the system reliability. In the case of a repairable system the availability becomes,

$$\boldsymbol{A(t) = 1 - F_T(t) - M_T(t).} \tag{2.2}$$

In the equation above, $M_T(t)$ is the distribution function for maintenance rate in time t. In general, safety concept relates to the control of recognized hazards in order to achieve a ''acceptable level of risk''. However, the term **SAFETY,** according to the CENELEC standards, is freedom from unacceptable risks, danger and injury from a technical failure in railways. The **RISK** of a hazard $R(H)$ is defined as the product of the probability (or likelihood) of a hazard $\Pr(H)$ and the consequences (such as fatality and costs) of a hazard$c(H)$:

$$\boldsymbol{R(H) = \Pr(H) \cdot c(H).} \tag{2.3}$$

The mathematical definition of risk is *expected adverse consequences* (Straub, 2011; Zio, 2007). The hazard is a physical situation, which has a potential for harm.

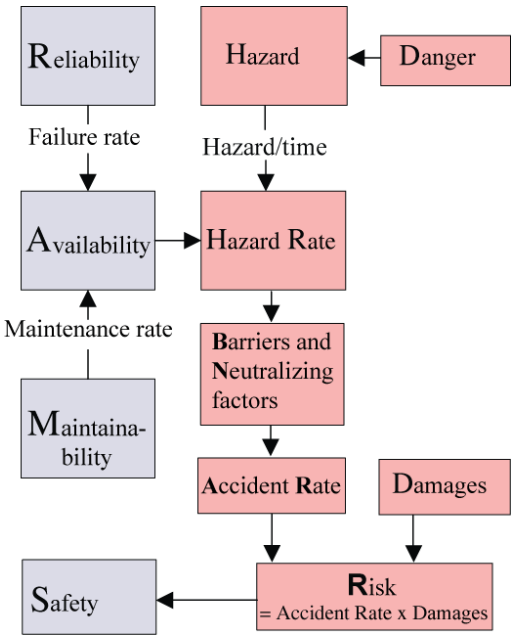


Figure 2.1: Interaction of RAMS components, after (Sapoznikov, et al., 2009)

Safety management in railway engineering systems is based on the combination of *reactive* approaches (like learning from accidents and mistakes) and *proactive* approaches (like risk and safety case analysis). This work focuses on the proactive approaches; therefore, mainly risk and safety case analysis will be dealt with here. *Risk assessment* is the process of identifying and analysing potential losses from a given failure in engineering systems such as railways. The risk assessment uses a combination of known information about the hazardous situation, knowledge about the underlying phenomenon or process and judgement about the information that is not certain or well understood. All unwanted situations – so-called hazards – are postulated and their consequences are modelled (Ericson, 2005; Mohaghegh, et al., 2009; Mahboob, et al., 2012(b); Podofillini, et al., 2006). The safety integrity requirements are then determined for the system, which is under different risks. Methods for risk analysis can be classified into three main categories (Ericson, 2005; Aven, 2008).

2.1.1 Simplified risk analysis

This is an informal procedure based on qualitative approaches. It establishes the risk picture using brainstorming sessions and group discussions. Group members are the expert in the field in which risk analysis is being carried out. The risk might be presented on a coarse scale, for example, low, moderate or high, making no use of formalized risk analysis methods.

2.1.2 Standard risk analysis

This is a more formalized procedure and includes both qualitative and quantitative approaches. In this analysis, more recognized methods such as Preliminary Hazard Analysis (PHA), Hazard and Operability (HAZOP) studies, Failure Modes and Effect Analysis (FMEA) and coarse risk analysis are utilized.

2.1.3 Model-based risk analysis

This is primarily a quantitative approach. Information obtained from the above two categories may be used in the development of a representation of the overall system in terms of logic diagrams, for example, Fault Tree, Reliability Block Diagram and Bayesian Networks.

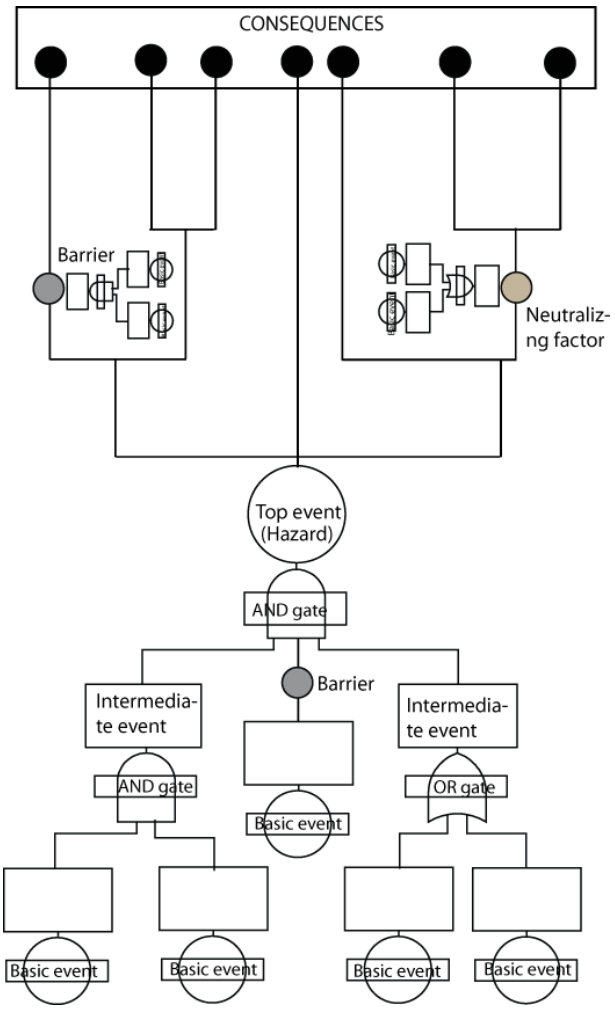


Figure 2.2: An example of a cause and consequence diagram.

The purpose of risk and safety assessment is to identify, determine and assess the risks present in a system. Systems can be engineering, social, natural and others. One way of determining and assessing risk is to utilize a cause and consequence diagram. For instance, Figure 2.2 shows a classical example of cause and consequence analysis where the hazard, also called the TE is located in the centre of the figure. This figure portrays the *Fault Symptom* approach where the fault represents the cause (lower part in Figure 2.2) and the symptom the consequence (upper part in Figure 2.2). There are barriers and neutralizing factors, which may prevent hazard occurrence and its propagation. There can be a large number of faults and symptoms in a cause and consequence diagram.

The causes of a TE can be failure in system components, human error and environmental effects. The consequences of a TE can be life safety risks to an individual person or society, environmental damages, structural damages or loss of production and services. Identification of the TE is an important task. Risk analysis has to identify the TEs and to develop the cause and consequence picture. How this is done depends on which method is adopted and how the results are utilized. However, the intent is always the same: to describe the risks in the system. Some methods used for railway risk and safety are briefly explained in the following.

2.2 Risk Matrix

This is also referred to as preliminary risk analysis. The risk matrix approach is mainly semi-quantitative. It becomes easy to use and understand, provided that the following main drawbacks of the risk matrix are resolved (Braband, 2010):

- calibration for particular application is required;
- the risk results are only valid for the system to which the risk matrices are applied; and
- the parameters (such as frequency and likelihood) are based on subjective definitions, which may lead to understanding complexities.

How analysis using risk matrix is performed is shown in the following three steps.

2.2.1 Determine the possible consequences

This step includes the impact of the TE, which is identified (by the system experts) during a preliminary hazard analysis. Each TE is described and ranked according to the severity of a consequence. Normally, the lowest and highest consequences are ranked one and five, respectively. Table 2.1 gives an overview describing and ranking the consequences of the TE. Here, the darker the colour the higher the severity of the consequence will be.

Table 2.1: An example of ranking the possible consequences.

Description Of event	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophe
Injury	Minor injury without first aid	Minor injury with first aid	Major injury, hospitalized	Long term incapacity, disability	Death, permanent incapacity
Service loss	Service suspension for one hour	Loss of service for 08 hours	Loss of service for one day	Loss of service for one week	Permanent loss of facility
Staffing and competence	Temporary loss in service (< 1 day)	Reduces service quality	Minor errors/defects	Serious errors/defects	Critical errors/defects

2.2.2 Likelihood of occurrence

Table 2.2 shows how the frequency and probability of occurrence are described subjectively and rankings are allotted to different categories of risks. Events data, brainstorming sessions and group discussions among the field experts determine how likely the consequences are to happen.

Table 2.2: Likelihood of occurrence.

Likelihood Score	Frequency	Probability
Rare	Not expected to occur for years	Expected to occur in exceptional circumstances
Unlikely	Expected annually	Unlikely to occur
Possible	Expected at least annually	Reasonable chance of occurring
Likely	Expected at least weekly	Expected in most circumstances
Almost certain	Expected daily	Most likely to occur than not

2.2.3 Risk scoring matrix

Risks are calculated by using the scoring matrix given in Table 2.3 where the definition of risk in Eq. (2.3) applies. Again, the darker the colour the higher the risk will be. Based on the risk analysis, management can now identify and rank mitigating measures/actions to prevent hazards. The risk-matrix-based analysis can highlight quite quickly the measures which might be implemented immediately in order to reduce the occurrence of a hazard or its consequences. In this way, the decision making on the adoption of safety measures can be facilitated.

Table 2.3: Risk calculation by using scoring matrix.

	Consequences				
Likelihood score	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophe
1. Rare	1	2	3	4	5
2. Unlikely	2	4	6	8	10
3. Possible	3	6	9	12	15
4. Likely	4	8	12	16	20
5. Almost certain	5	10	15	20	25
1-3 is Low; 4-6 is Moderate; 8-12 is High; 15-25 is Extreme					

2.3 Failure Modes & Effect Analysis – FMEA

FMEA is a bottom-up approach in analysing the effects of potential failure modes in an engineering system (Recht, 1966). It is a relatively simple method to determine possible failures and to predict the failure effects on the system. Investigation is carried out as to what happens if a particular component fails. The method represents a systematic analysis of the components of the system to identify all significant failure modes and to see how important they are for the system's safety and performance. Only one component is considered at a time, and it is assumed that other components are working at the same time. In this way, FMEA is not suitable for determining critical combinations of component failures.

Failure Modes, Effects and Criticality Analysis (FMECA) is an extension of FMEA. If criticality ranking for various failures in FMEA is added, we obtain a complete form of FMECA (Stewart & Melchers, 1997). The criticality is a function of the failure effect and the frequency or probability. The difference between an FMEA and an FMECA is not distinct, and sometime experts dealing with risk analysis do not distinguish between these two types of analysis (Aven, 2008). They also use criticality ranking as a part of FMEA. In order to ensure systematic study of the technical system, a specific FMECA form (see Table 2.4) is used for this purpose.

2.3.1 Example application of FMEA

A number of factors must be considered carefully before the implementation of an FMEA. For example, examination of each possible failure mode, costs/benefits of FMEA and its implementation, engineers' approval and decision making on the basis of risk criticality are important (Dhillon, 2011). In the following example of a rail sleeper, we also use the term FMEA when the analysis includes a ranking of criticality. A schematic representation of the ballasted railway track is shown in Figure 2.3.

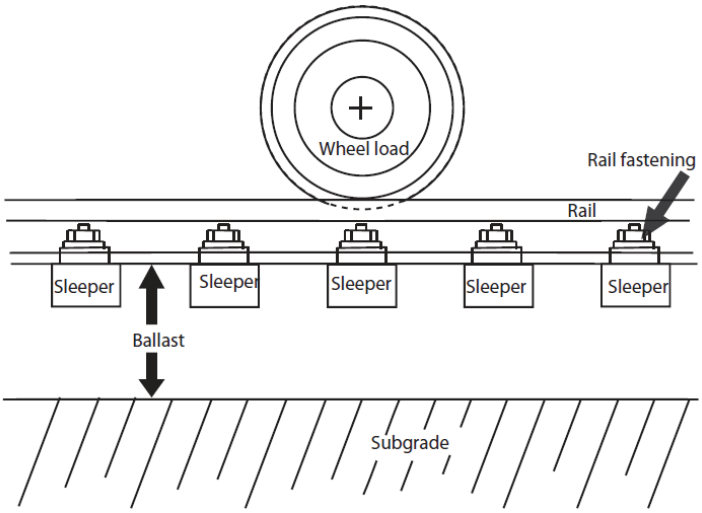


Figure 2.3: Components of the ballasted track.

The main function of the rail sleeper is to provide a durable guarantee of rail gauge, rail inclination and handling for all types of loads activated by vehicles. It also provides resistance during the thermal changes in the rail and transfers the load into the ballast bed and substructure (Ford, 2001). Rail sleepers can create hazards when they do not perform their function of supporting the rail and train load. An FMEA for the specific failure mode, load not supported by the sleeper, is presented in Table 2.4 and the general descriptions of the columns are explained below.

Identification (Column 1): Description of the specific component is given here. Name and/or part number of the specific component is also common referring to a system drawing or a functional diagram.

Function (or operational state) (Column 2): The intended function of the component, that is its working tasks in the system during the normal operation of the system, is briefly described. Similarly, other working modes such as stand – by mode are also mentioned here.

Table 2.4: Example of FMEA – damage to rail sleeper.

Identification	Function	Failure modes	Effect on other units in the system	Effect on system	Failure frequency	Ranking	Comments
Name: Rail sleeper for ballasted track. **Type: B70**	Handling of loads activated by train Durable guarantee of gauge.	Sleeper does not support load.	Shift of load on neighbouring track components.	Deflection rises in track. Increased vibrations in track & train. Rise in horizontal and vertical forces.	1/year. 3% of total number of load demands. 1/month. 1% of total load demands.	4 2 3 1	All other track components such as rail fastening and sub-grade are working fine.

Failure modes (Column 3): The ways the component fails to perform its functions are listed here. Only the failure modes that can be observed from outside are accounted for here, for example, the rail sleepers not transferring the load to the ballast and sub grade on demand (when a train is passing) is an observable failure mode. The internal failure modes are to be considered as failure causes, for example, corrosion of the reinforcement in the sleeper is responsible for the breakage of the sleeper which cannot withstand the load. All possible causes are listed in a separate column.

Effect on other units in the system (Column 4): Another column is used to note the effects of the specific failure mode of one component on other components in the system. Identification of failure propagation in the system due to one failure mode is emphasized: for example, the increased load on the neighbouring rail sleepers (that are supporting a common rail load) if one sleeper is damaged.

Effect on system (Column 5): Here one describes how the system is influenced by the specific failure mode. The operational state of the system as a result of a specific failure mode is expressed: for instance, whether the railway operation is intact, suspended or changed to another operational state after the failure.

Failure frequency (or probability) (Column 6): Here we assign the frequency for the specific failure mode and its consequence. Total frequency and relative frequencies for the different failure modes may be noted instead of noting the frequencies for all the different failure modes.

Failure effect (consequence) ranking (Column 7): Different failures are ranked according to their effects on safety, the possibilities of mitigating the failure, the length of the repair time, the production loss, and so forth. One way of ranking is to assign numbers to the effects, as shown in Column 7 of Table 2.4.

Comments (column 8): Assumptions and suppositions during the FMEA process are mentioned in this column.

2.4 Fault Tree Analysis – FTA

The common technique used in the schematic representation of a system is FTA, which is a deductive analysis. This method was developed by Bell Telephone Laboratories in 1962 when they performed a safety evaluation of the Minuteman Launch Control System (Vesely, et al., 1981). The Boeing Company has further developed the technique and made use of computer programs for both qualitative and quantitative FTA analysis for their systems. FTA is a top-down approach, which uses a tree structure to find the logical combinations of causes of a TE (Andrews & Moss, 1993; Aven, 2011; IEC 61508, 2000). A fault tree, see Figure 2.4, includes symbols that show the basic events of the system, and the relation between these events and the state of the system. The graphical symbols that show the relation are called *logical gates*. The output from a logical gate is determined by the input states. The system is analysed in the context of its functional and safety requirements and environmental conditions.

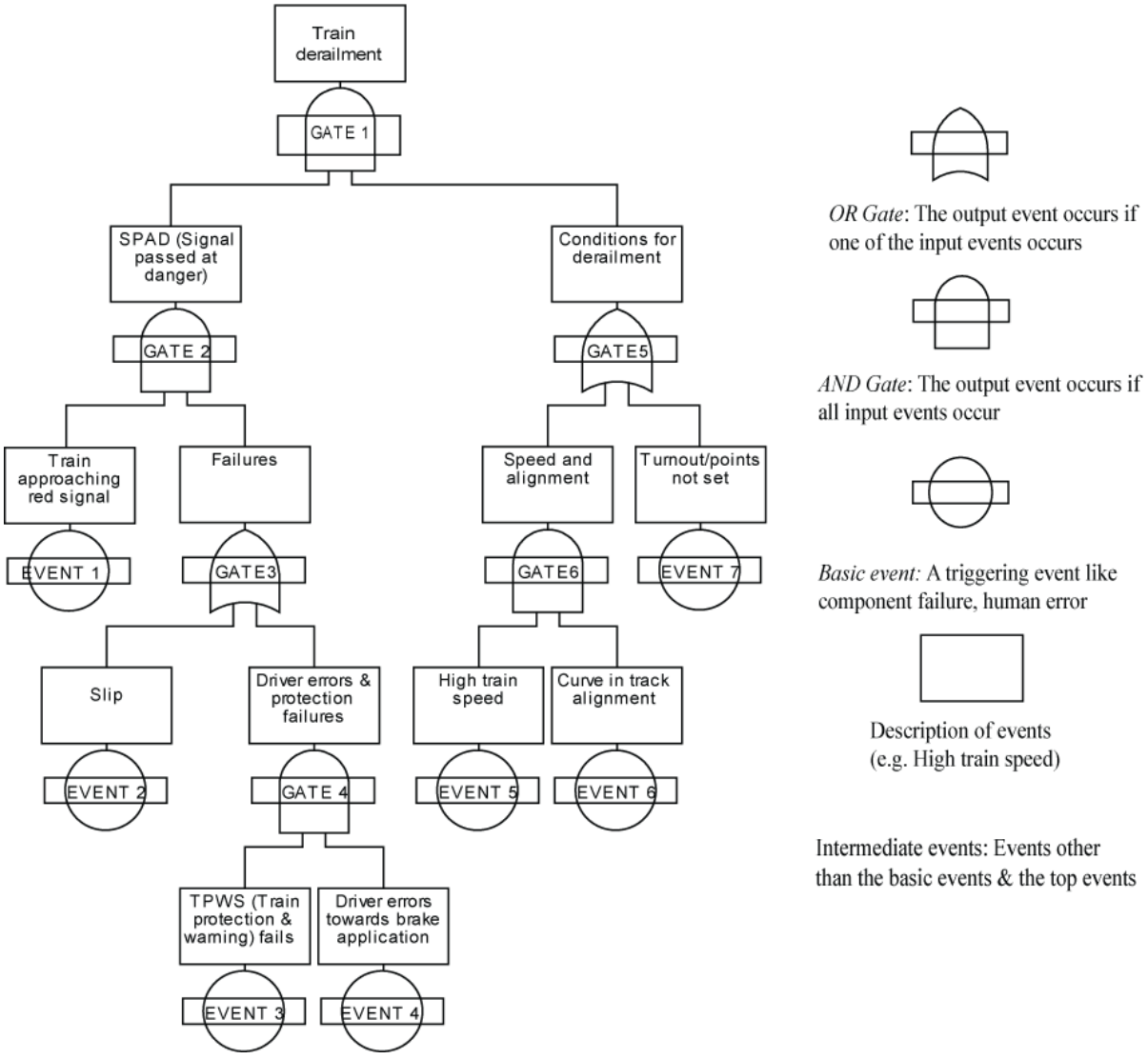


Figure 2.4: A Fault Tree for Train derailment (Mahboob, et al., 2012(c)).

In FTA, all combinations of basic events leading to the TE are identified. For example, the TE in Figure 2.4 is *Train derailment* and one basic event might be *High train speed*. The basic events are linked to the TE, through intermediate events, by logical gates. A basic event does not necessarily represent a pure component failure. The basic events may include items such as hardware, various sub-systems, environmental factors, human error or some social matters. The fault trees are constructed by repeatedly asking questions similar to

"What can be the causes of the TE?" Further progress in the causal relationship between the basic and intermediate events is stopped when we have reached the desired level of detail. Fault trees are dependent on the local conditions of the system; therefore, it is essential to think locally, and develop the fault tree using a systematic approach.

A standard FTA involves the following steps.

- Understand the system design and operation through data, drawings, procedures, diagrams, and so on.
- Define the problem and establish the correct TE (undesired events) for the analysis.
- Define the system rules and boundaries. What is included and what cannot be included?
- Follow the rules, boundaries, and logic (OR, AND,...) to build the FT model.
- Generate cut sets and compute probability values for the cut sets.
- Identify weak links and safety problems in the design and operation.
- Validate the FT model: check if the FT model is correct, complete, and accurately reflects system design and operation. Modify the FT if necessary during validation.
- Document the entire analysis with supporting data.

A cut set in the FTA is a group of basic events whose combined occurrence can cause the TE to occur. A cut set will be minimal if it cannot be reduced further and still promises the occurrence of the TE. Each minimal cut set is viewed as a parallel system of its components and the overall system state is viewed as a series system of the minimal cut sets. The basic assumptions of the standard FTA include (1) the events in FTA represent random variables with binary states (occurring/not occurring) and (2) basic events are statistically independent. In general, the probability of TE ($\Pr(TE)$) in the FT is computed as the function of the minimal cut sets by using the inclusion and exclusion principle in Eq. (2.4).

$$\mathbf{Pr}(\boldsymbol{TE}) = \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \mathbf{Pr}(\boldsymbol{C_i}) - \sum_{\boldsymbol{i=2}}^{\boldsymbol{n}} \sum_{\boldsymbol{j}}^{\boldsymbol{i-1}} \mathbf{Pr}\big(\boldsymbol{C_i} \cap \boldsymbol{C_j}\big) + \cdots + (\boldsymbol{-1})^{\boldsymbol{n-1}} \cdot \mathbf{Pr}(\boldsymbol{C_1} \cap \boldsymbol{C_2} \ldots \cap \boldsymbol{C_n}). \quad (2.4)$$

In the equation above, $\Pr(C_{\mathrm{i}})$ denotes the probability of the occurrence of minimal cut sets i in an FT and n is the number of minimal cut sets. For instance, the cut sets in the FT in Figure 2.4 are $(E_1 \cap E_3 \cap E_4 \cap E_7)$, $(E_1 \cap E_3 \cap E_4 \cap E_5 \cap E_6)$, $(E_1 \cap E_2 \cap E_7)$, $(E_1 \cap E_2 \cap E_5 \cap E_6)$. In the cut set representation above, we denote basic events in the FTA with their first letter, say E_1 for basic event 1. The total number of events in a cut set is called the order of the cut set. At least $2^{\mathrm{n}-1}$ terms need to be calculated in order to calculate the $\Pr(\mathrm{TE})$. In this way, the solution becomes computationally demanding when n increases. To avoid computational complexities the disjoint sum of the minimal cut sets is also used

$$\mathbf{Pr}(\boldsymbol{TE}) = \mathbf{Pr}(\boldsymbol{C_1}) + \mathbf{Pr}(\overline{\boldsymbol{C_1}})\,\mathbf{Pr}(\boldsymbol{C_2}) + \cdots + \mathbf{Pr}(\overline{\boldsymbol{C_1}})\,\mathbf{Pr}(\overline{\boldsymbol{C_2}}) \ldots \mathbf{Pr}(\overline{\boldsymbol{C_{n-1}}})\,\mathbf{Pr}(\boldsymbol{C_n}). \quad (2.5)$$

In the equation above, $\Pr(\overline{C_1}) = 1 - \Pr(C_1)$.

2.5 Reliability Block Diagram – RBD

A fault tree comprising only of AND and OR gates can be represented by an RBD. The RBD is also a graphical representation showing how component reliability can lead to the success or failure of a technical system. The graphical framework consists of blocks, which correspond to the components (or failure events) in the system, connected in series or parallel. The RBD can specify various combinations of components that can lead to a specific state or performance level of the system. The RBD equivalent to the FT in Figure 2.4 is shown in Figure 2.5.

It can be seen that the RBD is a combination of parallel and series systems. For a parallel system, all components must fail for the system to fail. Conversely, in a series system, all components must function for the successful operation of the system. In other words, the weakest element in the series system will be the strength of the overall system. The same

applies to the FTA. In the quantitative analysis, we calculate (1) the probability that the TE will occur and (2) the criticality of the basic events in the RBD and FT. To compute the TE probability we compute the failing probability for each minimal cut set, and then sum over all cut sets.

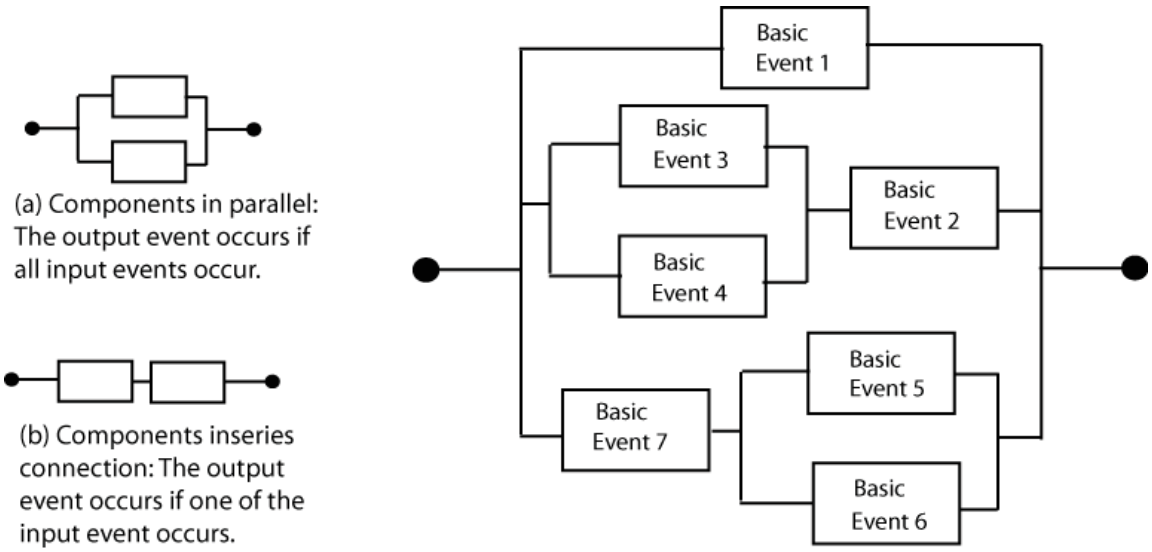


Figure 2.5: Reliability block diagram for train derailment due to signal passed at danger.

One can utilize FT or RBD methods if the system failure only depends on the combinations of its component failures. Both methods will lead to the same results for all static coherent system structures. A variety of algorithms exists for determining the minimal cut sets in an FT and RBD (Vesely, et al., 1981; NASA, 2002; Xing & Amari, 2008). A simple FT and RBD can be evaluated manually; however, large and complex FTs and RBDs require the aid of computerized methods for their evaluation. A problem with the qualitative analysis of a RBD (and FT) is that the qualitative approach misleads about the failure modes. For instance, there can be a case that larger cut sets have a higher failure probability than smaller ones. Therefore, quantitative analysis is often required for careful analysis.

2.6 Event Tree Analysis – ETA

ETA is an inductive analysis. It is used to determine the consequences of the TE. The event scenarios originate from the TE and then branch outwards following possible progressions of subsequent (failure) events. A number of possible consequences may arise from the TE. These may include damage to property, life risks and economic losses. Figure 2.6 shows an example of an ETA where life safety risks arising from PSD are modelled when a train is departing a platform (Mahboob, et al., 2013). Here, a set of scenarios is generated from the tree branches.

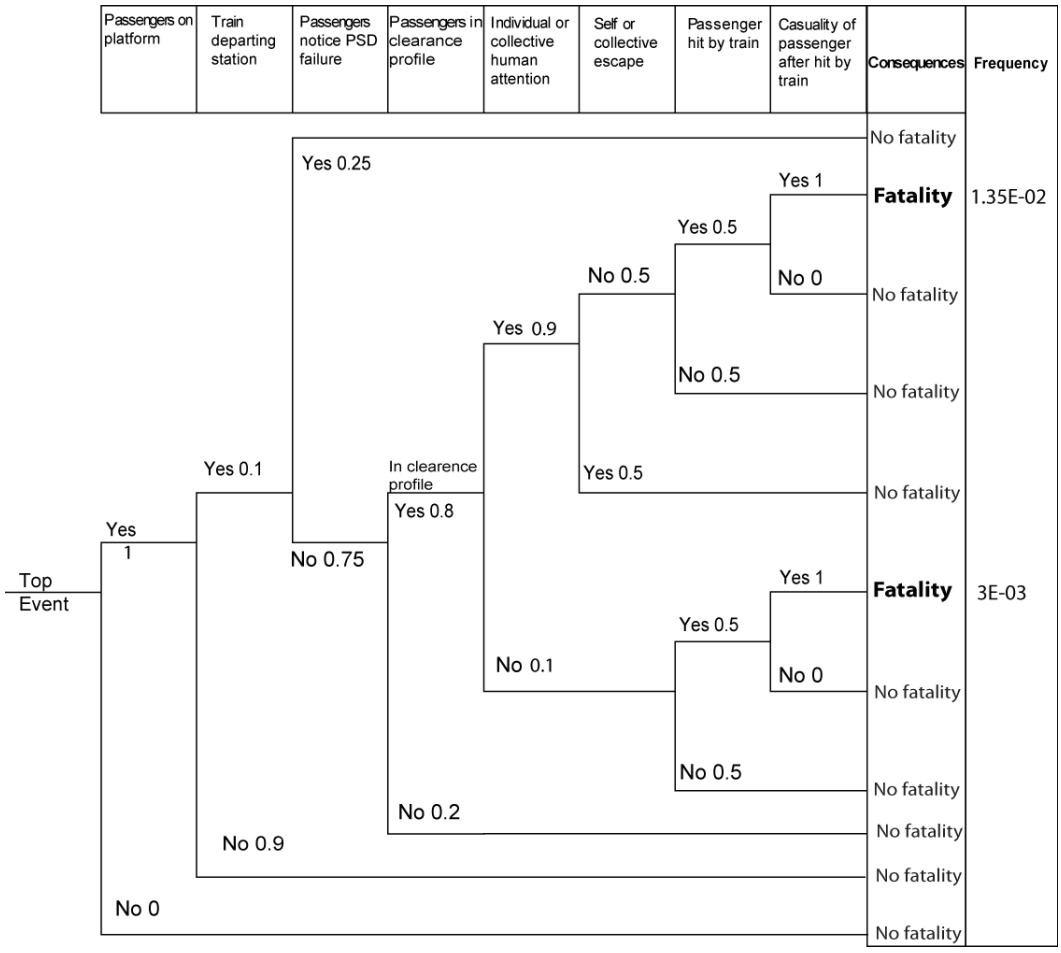


Figure 2.6: A sample Event Tree analysis for Top Event '' Wrong opening of platform screen doors when train is departing'' (Mahboob, et al., 2013).

It is common to pose the branch questions in such a way that the answers to all the branches' questions are yes or no. In this way, two scenarios will come out, the best at one end and the worst at the other. Finally, the consequence matrix is drawn, which describes the consequences arising from each terminating event. In Figure 2.6, the consequences are restricted to the (frequencies of) fatalities. In the quantitative analysis of the ET, frequencies (or probabilities) are linked to the various event scenarios and their consequences. It should be mentioned that definitions of the cut sets are also applicable to ETs. The probability of each consequence is computed by multiplying the probability of the initiating event (that is TE in the FTA) with the probabilities of the events defining each scenario. For example, one of the probabilities of fatality $1.35 \cdot 10^{-02}$ in Figure 2.6 is calculated by multiplying $1 \cdot 0.1 \cdot 0.75 \cdot 0.8 \cdot 0.9 \cdot 0.5 \cdot 0.5 \cdot 1$.

2.7 Safety Risk Model – SRM

For systems in which accidents are frequent such as highways the statistical analysis of past accidents is carried out by estimating quantities such as λ (e.g. failure rate) and μ (e.g. arrival rate) that are not directly observable. For systems such as railways or aviation, in which accidents are much less frequent and have more variable outcomes, statistical analysis of the data is still possible, but the precision of the estimates of the parameters is much lower. For systems in which accidents are very rare and accident data is so small in number, direct statistical analysis of accident data is of little help in estimating the risk. In this case risk models are developed which are specific to the system, and estimate risks by modelling both the precursor and potential consequences of the hazards. For some systems, the risks are estimated by both of the above methods in a model called SRM or Bow-Tie model. The SRM is a large scale fault-tree and event-tree based model used to assess risk in engineering systems. In railways, the SRM was first applied to assess the risk in the mainline railways in the UK (RS, 2001). The main objective of this SRM was to develop a basic understanding of the nature and information of the current risks relating to the mainline railways in the UK. The model consists of 120 hazardous events and over 4000 consequences that collectively determine the mainline railway risks. The base event probabilities are determined from the historical data of accidents and incidents. In this way, SRM averages the network-

wide risks; however, it does not profile the risk in different locations because the causes of varying base event probabilities are not part of the model (RSSB, 2011). The Irish railway has also developed a parameterized risk model (Sotera, 2006). This model consists of fault trees and event trees for all possible accident sequences on the entire Irish railway network. The infrastructure and environment factors (such as degree of curvature, rail gauge, rail condition) are parameters in this model. Over 200 parameters are included in the model and a set of values for these parameters is calculated at 227 separate locations. Cut sets generated from the fault trees are evaluated for different parameter values at each location. A parameterized risk model, developed by the Irish railway, can identify risk by location, by rail type and so on.

Another example of the SRM is ROSA (Rail Optimization Safety Analysis), which is under development for the German railway network (IRSC, 2008). A schematic representation of the ROSA-based safety project is shown in Figure 2.7 where the complete railway network will be considered through its boundary definitions, that is, operation, maintenance and traffic. A complete list of hazardous events, so called initiating points will be established at a generic level. This generic list is independent of the actually implemented safety measures and functions. Possible consequences of each of the hazardous event will be analysed by using an ET.

In Figure 2.7, the ROSA model has barriers in the upper and lower parts of the pyramid, or bow-tie diagram. In the lower part, barriers are introduced to prevent the hazardous events. These are the (probability) reducing or preventive barriers. On the upper side of the SRM there are barriers which prevent the propagation of the hazardous event. The cause and consequence diagram in Figure 2.2 is also a kind of SRM, but on a smaller scale.

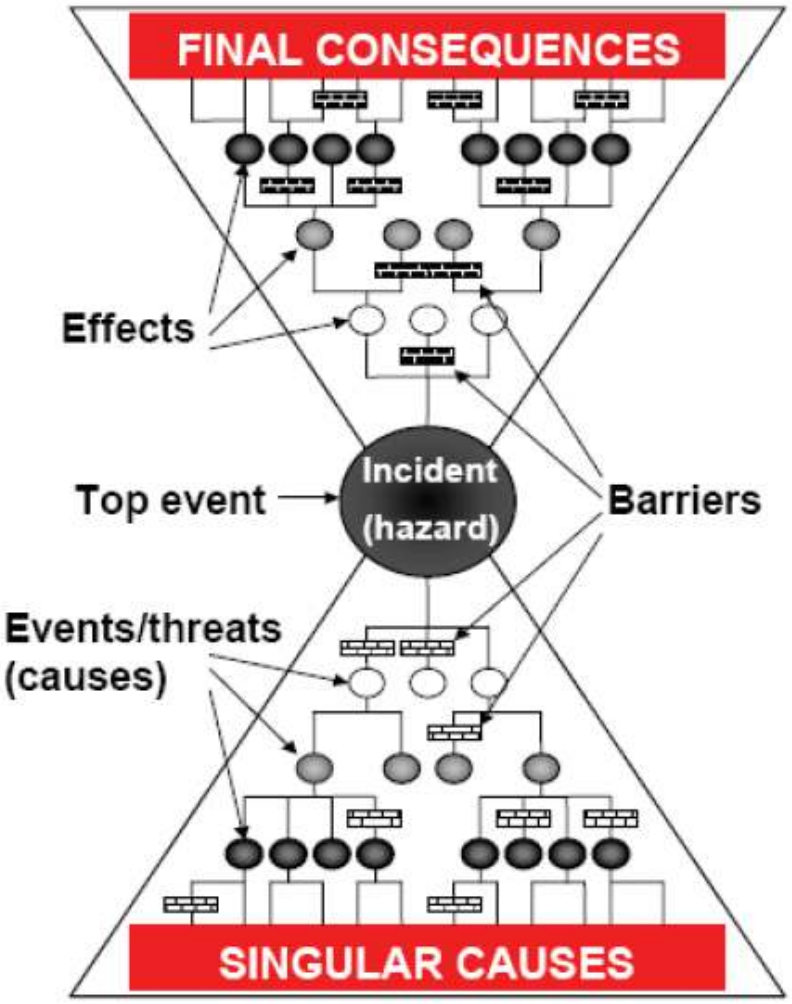


Figure 2.7: Safety risk model or Bow-Tie model ROSA (Puettner & Geisler, 2008).

2.8 Markov Model – MM

MM is used to compute the probability that the system is in a specific state at a given time, for all possible states and times. For example, the probability that the system (represented by Figure 2.8) will attain state 3 (Unsafe, Unavailable) be computed using MM. Accidents can occur if the system enters into state 3; meaning that no freedom from unacceptable risks. MMs are based on Markov processes (MP). An MP is a stochastic process $\{X(t); t \geq 0\}$, which is governed by the transition probabilities. An MP is completely characterized by its initial states and transition states. Therefore, the two main concepts – system states and

transition states – in the MM are very important. The system state represents the system at any given instant of time. The transition states govern the changes of a state that occur within a system. Solving an MM requires solving a set of differential equations such as

$AP(t) = P'(t)$.

The specific representation is:

$$\begin{bmatrix} -\boldsymbol{A_{00}} & \cdots & \boldsymbol{A_{ON}} \\ \vdots & \ddots & \vdots \\ \boldsymbol{A_{N0}} & \cdots & -\boldsymbol{A_{NN}} \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{P_1(t)} \\ \boldsymbol{P_2(t)} \\ \boldsymbol{P_3(t)} \end{bmatrix} = \begin{bmatrix} \boldsymbol{P'_1(t)} \\ \boldsymbol{P'_2(t)} \\ \boldsymbol{P'_3(t)} \end{bmatrix}. \tag{2.6}$$

In the equation above A_{jk} , $j \neq k$ is the transition rate form state j to state k. The diagonal element A_{jj} in the matrix A is the sum of departure rates from state j. In this way,

$$\boldsymbol{A_{jj}} = \sum_{\boldsymbol{k=1,k\neq j}}^{\boldsymbol{n}} \boldsymbol{A_{jk}} . \tag{2.7}$$

In matrix A above, the sum of each column becomes 0. The probability of system failure is calculated by adding the probability of being in each failure state. If $P_{F_i}(t)$ is the failure probability of the system in state F_i at time t then the system level failure probability will be calculated as

$$\sum_{\forall \boldsymbol{F}} \boldsymbol{P_{F_i}(t)} . \tag{2.8}$$

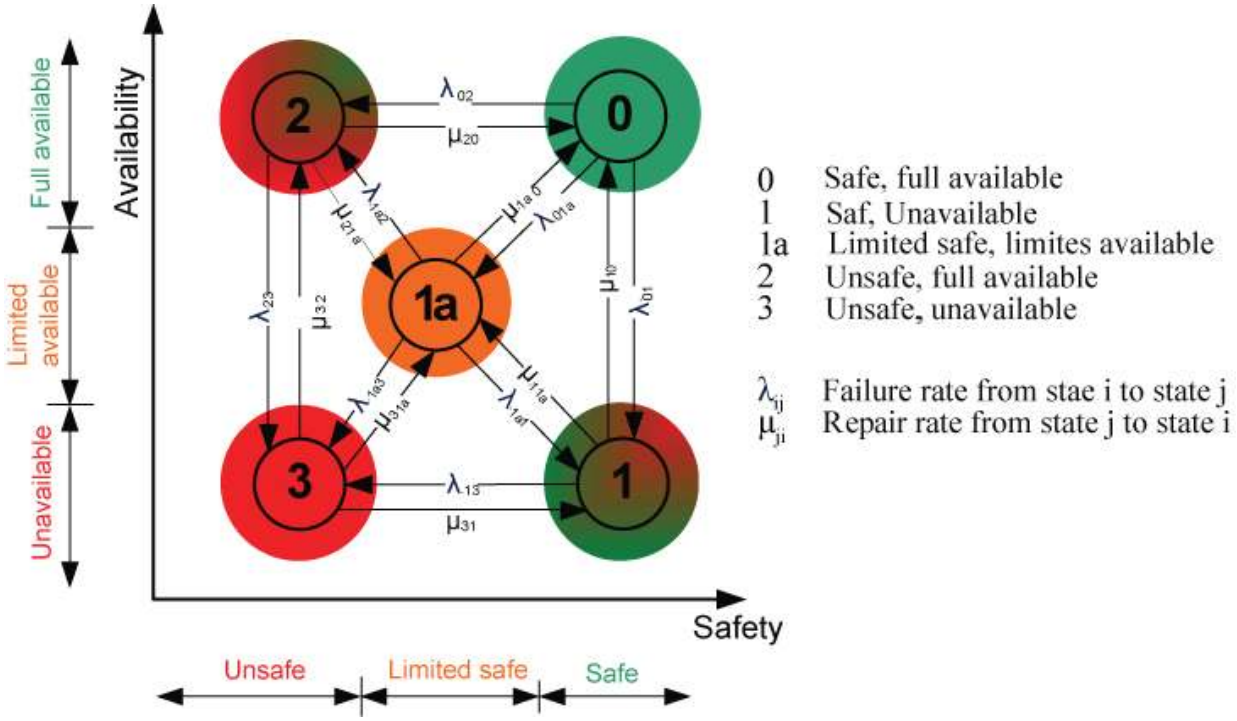


Figure 2.8: A Markov Model for system safety and availability, after (Anders, 2008).

Markov chains, which facilitate modelling of discrete stochastic processes, are special instances of an MP. These are based on Markov property: the knowledge of the system state at a future stage is independent of the knowledge of the current system stage. In other words, the Markov property holds as along as the following holds:

$$\boldsymbol{p}(\boldsymbol{x_n} \mid \boldsymbol{x_0}, \boldsymbol{x_1}, \dots, \boldsymbol{x_{n-1}}) = \boldsymbol{p}(\boldsymbol{x_n} \mid \boldsymbol{x_{n-1}}). \tag{2.9}$$

In the equation above, $p(x)$ represents the probability mass function of a discrete random variable X (that corresponds to the system state) at different time steps. Markov chains are described by initial probabilities $\mathbf{q}$ and transition probabilities or the transition matrix $\boldsymbol{\pi}$. In homogenous Markov chains, the transition probabilities are the same for all the transitions. In order to illustrate the use of Markov chains in railways risk, let us consider the following example application. Let $X_{(n)}$ represent the condition of a (non-repairable) railway facility at time step n. ($n = 1, 2, \dots$ the number of years following the installation.) The initial probabilities of the four system states at the beginning of service life are

$$\boldsymbol{q_0} = \begin{bmatrix} \textbf{1. Safe and full available} \\ \textbf{2. Safe and unavailable} \\ \textbf{3. Unsafe and full available} \\ \textbf{4. Unsafe and Unavailable} \end{bmatrix} = \begin{bmatrix} \mathbf{0.95} \\ \mathbf{0.03} \\ \mathbf{0.02} \\ \mathbf{0} \end{bmatrix}. \tag{2.10}$$

In the equation above, the system states 3 and 4 can cause risks on railways and their probabilities are changing w.r.t time. The transition probability matrix $\boldsymbol{\pi}$ that governs the changes of a state that occur within a system is

$$\boldsymbol{\pi} = \begin{bmatrix} \boldsymbol{\pi_{11}} & \boldsymbol{\pi_{12}} & \boldsymbol{\pi_{13}} & \boldsymbol{\pi_{14}} \\ \boldsymbol{\pi_{21}} & \boldsymbol{\pi_{22}} & \boldsymbol{\pi_{23}} & \boldsymbol{\pi_{24}} \\ \boldsymbol{\pi_{31}} & \boldsymbol{\pi_{32}} & \boldsymbol{\pi_{33}} & \boldsymbol{\pi_{34}} \\ \boldsymbol{\pi_{41}} & \boldsymbol{\pi_{42}} & \boldsymbol{\pi_{43}} & \boldsymbol{\pi_{44}} \end{bmatrix} = \begin{bmatrix} \mathbf{0.85} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0.15} & \mathbf{0.9} & \mathbf{0.1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0.0.5} & \mathbf{0.8} & \mathbf{0} \\ \mathbf{0} & \mathbf{0.05} & \mathbf{0.1} & \mathbf{1} \end{bmatrix}. \tag{2.11}$$

In the equation above, π_{jk} , $j \neq k$ is the transition rate from state j to state k. For example, π_{32} is the transition probability of the system in state 3 at time step n given that it was in state 2 in time step $n-1$. The probability of system failure as a function of time is shown in Figure 2.9. If one is interested in the failure probability distribution of the railway system after 25 years, it will be calculated in the following way:

$$\boldsymbol{q_{25}} = \boldsymbol{\pi^{25}} \boldsymbol{q_0} = \begin{bmatrix} \mathbf{0.0163} \\ \mathbf{0.2425} \\ \mathbf{0.0791} \\ \mathbf{0.6621} \end{bmatrix}. \tag{2.12}$$

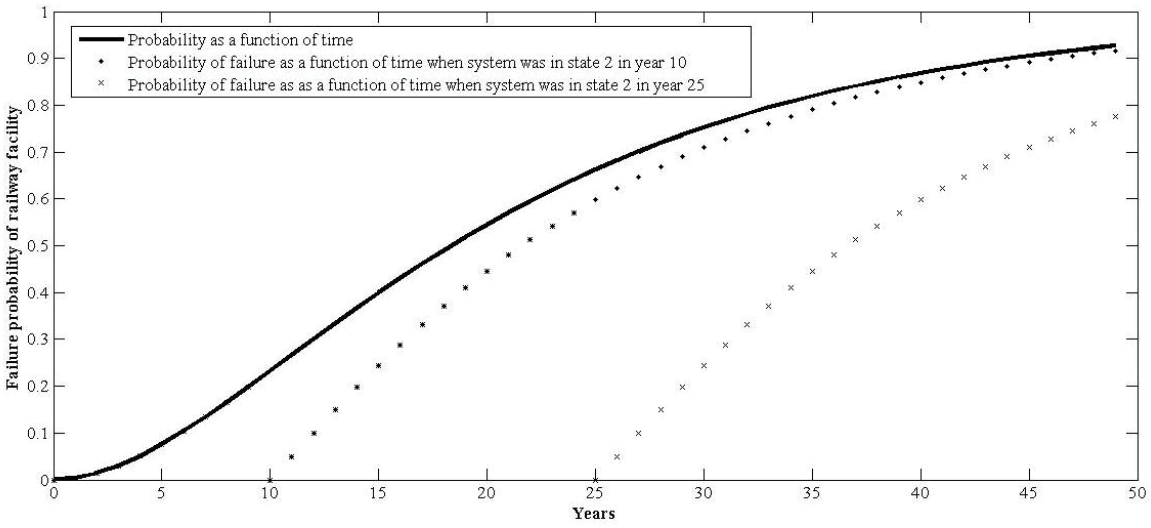


Figure 2.9: Failure probability of (non-repairable) railway facility as a function of time.

2.9 Quantification of expected values

Risks are present in the system whenever there is uncertainty in the system. Quantities whose values are unknown to us are called random quantities or uncertain quantities. Uncertain quantities can be due to randomness (aleatory) or due to incomplete knowledge (epistemic) of the system or process (Lindley, 1982a; Singpurwalla, 2006; Bernardo & Smith, 2000; Stewart & Melchers, 1997). The estimation of uncertainty requires the quantitative description of both the frequency and the performance of the system elements which are causing system risks. The quantitative description of the performance, for example, for individual elements is a variable. It can be a point estimate (e.g. mean failure rate) or a random variable (e.g. probability distribution of failure rates). Some system variables are categorized in the following way:

- resistance, capacity and strength of the different engineering systems;
- load and stress demands placed on the system;
- human reliabilities, for example, human error rates; and
- consequence of failure rates, for example, economic loss, life loss, structural damage, property losses and so forth.

A point estimate such as the mean value has a single numerical value, which is used to describe the best estimate of the value of the variable. For example, when fatal accidents are estimated as 2.1 per billion train-km for UK railways (Evans, 2003), this value is a point estimate. Point estimates for variables ignore variability (Bowles, 2002). For instance, the fatal accident rate is not the same for all similar sections of the UK's railways due to different environment, load and maintenance conditions. However, it is assumed to be the same for all sections at any time during the life of the system in point estimates. Another cause of variability is uncertainty in the field data due to the lack of understanding of the system, obsolescence and so forth. In order to address the variability and uncertainty issues in the data for the purposes of risk analysis, one should represent variables such as resistance, load and consequences as random variables, which are characterized by probability distributions. In this way, for instance, random variables will distribute the variation in fatal accidents evenly among similar sections of the UK's railways.

Random variables are described by probability distributions. Probability density function (PDF), probability mass function (PMF), and cumulative distribution function (CDF) are the forms of probability distributions for random variables. In probabilistic modelling of random variables, a functional form (e.g. Poisson distribution or binomial distribution) is selected and the values of its parameters are determined. The well-known statistical parameters used to describe probabilistic models are first moment (mean, μ_X) and the second moment (variance, σ_X^2). The mean provides the best estimates of the value of a random variable, that is the most likely to occur in practice, whereas, variance provides a measure of uncertainty associated with this random variable. The simplest way of computing the moments of a probabilistic model for discrete (Eq. (2.13)) and continuous (Eq. (2.14)) cases are given in the following.

$$\mu_X = \sum_{all\ x_i} x_i\, p_X(x_i) \quad , \quad \sigma_X^2 = \sum_{all\ x_i} (x_i - \mu_X)^2 . p_X(x_i) \tag{2.13}$$

$$\mu_X = \int_{-\infty}^{\infty} x\, f_X(x)\, dx \quad , \quad \sigma_X^2 = \int_{-\infty}^{\infty} (x - \mu_X)^2 . f_X(x)\, dx \tag{2.14}$$

In the equations above, $p_X(x_i)$ is the probability of the occurrence of each value x_i of the random variable X and $f_X(x)$ is the PDF for the continuous random variable case. Other measures are the standard deviation σ_X and the coefficient of variance $V_X = \frac{\sigma_X}{\mu_X}$. The standard deviation shows how much variation there is from the mean whereas V_X is a normalized measure of the dispersion of a probability distribution. The third moment, skewness, of the probability distribution provides information about the asymmetry. For further details on the description and characterization of various random variables see (Benjamin & Cornell, 1970; Ross, 1997) and for their application to risk, safety and reliability see (Rausand & Hoyland, 2004; Zio, 2007; Kottegoda & Rosso, 2008; Misra, 2008).

Different probability distribution models, for example, binomial, exponential, Poisson, normal, lognormal, gamma, extreme values for maxima and minima, beta, and others, have been developed and are used based on the characteristics of the system elements. The 'moments' are the parts of the parameters for different distribution models above. The selection of probability distribution for the purpose of risk analysis is dependent upon the characteristics of the random variables and the relation by which the risk analyst prefers to describe it. Some commonly used probability distributions in engineering risk and reliability are given in (Faber, 2012; Bucher, 2009; Straub, 2011). For example, the (2-parameter) Weibull distribution is widely used for modelling lifetime distributions in engineering. The PDF of Weibull is given by:

$$\boldsymbol{f_T(t) = \frac{\beta}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1} \exp\left(-\frac{t}{\alpha}\right)^{\beta}; \quad t \geq 0, \alpha \geq 0, \beta > 1} \tag{2.15}$$

In the equation above, α and β are the scale and the shape parameters, respectively. In the literature, α is referred to as the characteristic life. One of the main reasons for this is the flexibility of the distribution shapes that can be approximated by varying Weibull's two parameters (α, β). For $\beta = 1$ in the Weibull PDF above, we obtain an exponential distribution, which is also widely used to model the amount of time until a specific event occurs or to

model the time between independent events. The PDF of an exponential distribution with arrival rate $\frac{1}{\alpha}$ in time t is calculated as

$$\boldsymbol{f_T(t) = \frac{1}{\alpha}\exp\left(-\frac{t}{\alpha}\right)\,;\quad t \geq 0\,,\alpha \geq 0\,.} \tag{2.16}$$

In this way, the first and second moments of an exponential distribution will be α and α^2, respectively.

Mainly, uncertainty in probabilistic models arises from two error sources: the model inputs and the models themselves (Benjamin & Cornell, 1970). The reasons for model uncertainty are: (1) the random variables for the model parameters and (2) the ability of the probabilistic models to fully describe the characteristics of the system and its elements. Model inputs cause statistical uncertainty which fails to estimate the model parameters with precision as they are estimated from a limited amount of data. (Fundamentally, we want more and more data for improved estimates.) These types of uncertainties can be eliminated by gathering sufficient data about the events and by making system understanding better. That is why statistical inference used for parameter estimation establishes probability models based on observations. Method of Moments (MOM), Maximum Likelihood Estimation (MLE) and Bayesian analysis (BA) are well-known statistical inference methods used to estimate the distribution parameters on the basis of data. MOM uses sample mean and variance as point estimators for the mean and the standard deviation of the random variable. This random variable describes the full population that is represented by the data set. When fitting a parametric distribution to a set of data, we equate the sample moments to those of the fitted distribution in order to estimate the distribution parameters (Kottegoda & Rosso, 2008). For instance, when a normal distribution ($N\sim(\mu_X, \sigma_X)$) is selected as the functional form of the probability model the point estimates for the distribution parameters μ_X and σ_X are simply $\bar{x}$ (mean of sample) and $\sqrt{S^2}$ (standard deviation of sample), respectively.

The MLE method is applied when a random variable X has a known PDF, $f_X(x)$ and observed values $x_1, \ldots, x_n$, in a random sample of size n. The likelihood function of unknown parameter θ is

$$\boldsymbol{L}\,(\boldsymbol{\theta} \mid \boldsymbol{x_1}, \boldsymbol{x_2}, \ldots, \boldsymbol{x_n}) = \boldsymbol{f}(\,\boldsymbol{x_1}, \boldsymbol{x_2}, \ldots, \boldsymbol{x_n} \mid \boldsymbol{\theta}\,) = \prod_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{f_X}(\boldsymbol{x_i}|\boldsymbol{\theta}). \tag{2.17}$$

The objective is to maximize $L(\theta)$ for the given data set. This is done by taking as many partial derivatives of $L(\theta)$ as is equal to the number of parameters in the model, and equating them to zero. At the end, the MLE of the parameter set θ are calculated from the solutions of the equations.

2.9.1 Bayesian Analysis – BA

When additional information becomes available, the probability structure in the model may be updated. This is done by using BA, which is based on Bayes' theorem (Gelman, et al., 2009; Koller & Friedman, 2009). This method is particularly useful when the amount of available data is sparse and the statistical uncertainty is large. In these cases, experimental data (obtained for a specific plant) and reliability data (obtained from reliability databases or expert opinions) are combined by using Bayes theorem. This theorem states how prior probabilities, combined with new information from a sample, can be used to update beliefs. The updated belief is called the posterior probability and is calculated as:

$$\boldsymbol{p}(\boldsymbol{\theta_j}|\boldsymbol{x}) \propto \boldsymbol{p}(\boldsymbol{x}|\boldsymbol{\theta_j})\boldsymbol{p}(\boldsymbol{\theta_j}) = \frac{\boldsymbol{p}(\boldsymbol{x}|\boldsymbol{\theta_j})\boldsymbol{p}(\boldsymbol{\theta_j})}{\sum_j \boldsymbol{p}(\boldsymbol{x}|\boldsymbol{\theta_j})\boldsymbol{p}(\boldsymbol{\theta_j})} = \frac{\boldsymbol{p}(\boldsymbol{x}|\boldsymbol{\theta_j})\boldsymbol{p}(\boldsymbol{\theta_j})}{\boldsymbol{p}(\boldsymbol{x})}\,. \tag{2.18}$$

In the equation above θ is the unknown parameter whereas

- $p(\theta_j)$ is the prior distribution of parameter θ_j which represents the data;
- x is a sample drawn from the underlying distribution which represents the experimental data;
- $p(x|\theta_j)$ is the sampling density of x and represents the likelihood function or conditional probability of observing the experimental outcome x given the value of the parameter θ. Our prior knowledge of the failure data is weighted

by the likelihood function, which is regarded as a credibility check on the prior knowledge;

- $p(\theta_j|x)$ is the posterior distribution of x; and
- $\sum_j p(x|\theta_j)p(\theta_j) = p(x)$ is a normalizing constant to satisfy the requirement for the resulting PMF.

DISCRETE FORM OF BAYES' THEOREM

A simple case of a discrete probability distribution, such as Poisson, is shown to demonstrate the use of Bayes' theorem. Let θ_j be one failure rate of a set of possible rates of a component and x is evidence. We wish to express our knowledge in terms of $p(\theta_j \mid x)$. We want to compute the $p(\theta_j \mid x =< 2{,}100 >)$, which is the probability of θ_j given the observation of 02 failures in a 100 hour operation:

$$\boldsymbol{p(\theta_j \mid x =< 2,100 >) = \frac{p(x =< 2,100 > |\theta_j)p(\theta_j)}{\sum_{j=1}^{5} p(x =< 2,100 > |\theta_j)p(\theta_j)}} \; . \tag{2.19}$$

Assuming that θ_j is a constant and the likelihood function follows the Poisson distribution:

$$\boldsymbol{p(x \mid \theta_j) = p(x =< 2,100 > |\theta_j) = \frac{(\theta_j \cdot t)^2 \exp(-\theta_j \cdot t)}{2!}}. \tag{2.20}$$

The calculation of the posterior probability of the desired event $p(\theta_j \mid x =< 2{,}100 >)$ for $t = 100$ hours is shown in Table 2.5. The comparison of the prior and the posterior knowledge is shown in Figure 2.10. It should be noted that the posterior probability of the desired event increases after updating.

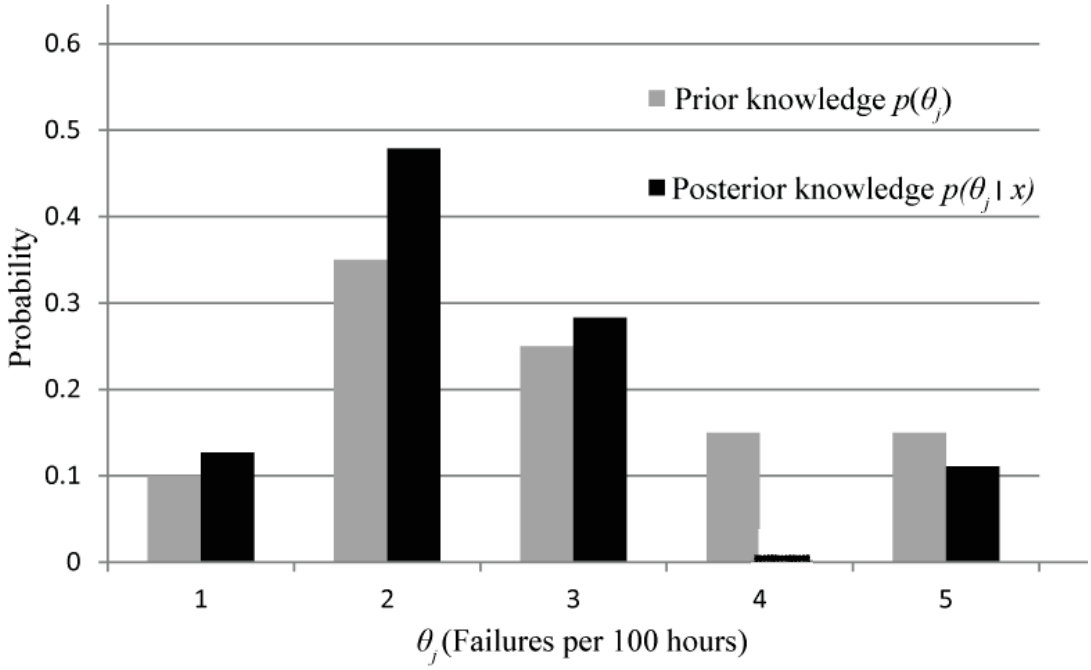


Figure 2.10: Comparison of the prior and posterior knowledge for the discrete case of Bayes' theorem.

Table 2.5: Discrete case of posterior probability.

j	θ_j	$p(\theta_j)$	$p(x \mid \theta_j)$	$p(\theta_j \mid x) \propto p(x \mid \theta_j) p(\theta_j)$	$p(\theta_j \mid x) = \frac{p(x \mid \theta_j) p(\theta_j)}{\sum_j p(x \mid \theta_j) p(\theta_j)}$
1	0.015	0.1	0.251	0.025	0.126
2	0.02	0.35	0.270	0.094	0.478
3	0.03	0.25	0.224	0.056	0.283
4	0.2	0.15	$4.12 \cdot 10^{-07}$	$6.18 \cdot 10^{-08}$	$3.12 \cdot 10^{-07}$
5	0.04	0.15	0.146	0.021	0.111
				$\sum_j p(x \mid \theta_j) p(\theta_j) = \mathbf{0.198}$	$\sum_j p(\theta_j \mid x) = \mathbf{1}$

CONTINUOUS FORM OF BAYES' THEOREM

The following example shows the application of Bayes' theorem as a continuous case. Authorities have approved a new railway facility for a town. Therefore, new infrastructure, including, among others, a station building, railway line and signals points needs to be built. It is important to ensure that the soil has sufficient strength to withstand the railway load (of passenger and goods trains) if the new line is constructed on it. The railway engineers are interested in the distribution of soil strength so that they can decide the maximum railway load. The soil experts decide that the prior distribution of strength θ is $N(80000, 1200^2)$ in metric units. They have carried out five random soil tests with mean strength of $75000\ \mathrm{N/m^2}$. If $x_1, x_2, \ldots, x_n$ is a random sample taken from a distribution $N(\theta, \sigma^2)$ with known σ^2 and the prior distribution of the mean θ is $N(\mu_0, \sigma_0)$, we get the posterior distribution of θ as (Kottegoda & Rosso, 2008):

$$(\boldsymbol{\theta} \mid \boldsymbol{x}) \sim \boldsymbol{N}\left(\frac{\boldsymbol{\sigma_0^2}\,\bar{\boldsymbol{x}} + \frac{\mu_0 \boldsymbol{\sigma^2}}{\boldsymbol{n}}}{\boldsymbol{\sigma_0^2} + \frac{\boldsymbol{\sigma^2}}{\boldsymbol{n}}}, \quad \frac{\frac{\boldsymbol{\sigma_0^2}\boldsymbol{\sigma^2}}{\boldsymbol{n}}}{\boldsymbol{\sigma_0^2} + \frac{\boldsymbol{\sigma^2}}{\boldsymbol{n}}} \right). \tag{2.21}$$

In the equation above, the posterior mean is the weighted average of the prior mean μ_0 and the sample mean $\bar{x}$ as n becomes very large. The prior, likelihood and posterior distributions are shown in Figure 2.11 where we consider that the standard deviation for the random sample is $15000^2\ \mathrm{N/m^2}$.

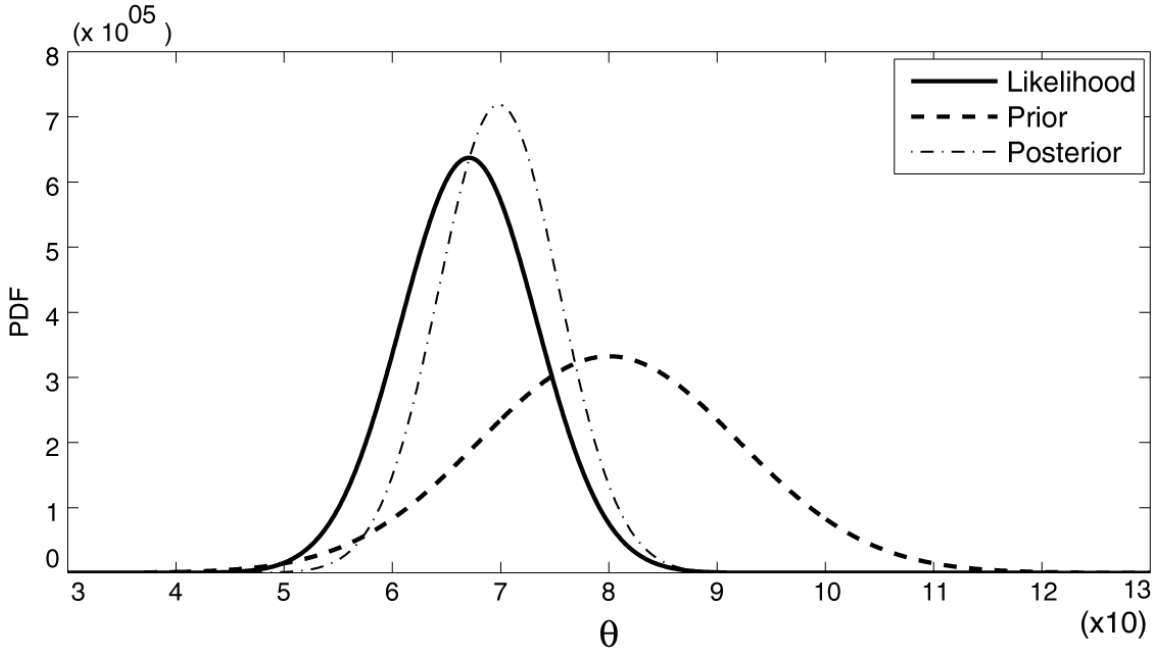


Figure 2.11: Prior, likelihood and posterior PDFs of soil strength for railway track.

2.9.2 Hazard Function – HF

HFs (or failure rate functions) are also applied in the fields of railway (Sapoznikov, et al., 2009) and transportation (Rashidi & Mohammadian, 2011). The HF expresses the propensity for a part to fail shortly after time t given that it has survived until time t, that is, that the probability of failing in the time interval $(t, t + \Delta t)$ assuming that the part has lasted until time t, is approximately $\Delta_t \cdot h(t)$. Let T be a random variable representing the time until a component fails. Let $F_T(t)$ and $f_T(t)$ be the CDF and PDF of T, respectively. The HF, denoted by $h_T(t)$ is defined by

$$\boldsymbol{h_T(t) = \frac{f_T(t)}{1 - F_T(t)} = \frac{f_T(t)}{R_T(t)}}\ , \qquad \boldsymbol{F_T(t) \neq 1.} \tag{2.22}$$

In the equation above, $R_T(t)$ is the reliability (or survival) function. An alternative form of the HF is

$$\boldsymbol{h_T(t) = \frac{-\frac{d}{dt}(R_T(t))}{R_T(t)}} \quad , \qquad \boldsymbol{F_T(t) \neq 1.} \tag{2.23}$$

By solving the differential equation above, we get $R_T(t)$ as the function of the $h_T(x)$ in the following exponential form:

$$\boldsymbol{R_T(t) = \exp\{-\int_0^t h_T(x)dt\}}. \tag{2.24}$$

To illustrate the effect of the $h_T(t)$ and $R_T(t)$, the 2-parameter Weibull distribution is used:

$$\boldsymbol{h_T(t) = \frac{f_T(t)}{1 - F_T(t)} = \frac{\frac{\beta}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1}\exp\left(-\frac{t}{\alpha}\right)^{\beta}}{1 - (1 - \exp\left(-\frac{t}{\alpha}\right)^{\beta})} = \frac{\beta}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1}}. \tag{2.25}$$

The $h_T(t)$ of the Weibull is shown in Figure 2.12 for different values of β and α. The Weibull HF has well-known properties that are:

- If $\beta < 1$, then the hazard rate decreases with time;
- If $\beta > 1$, then the hazard rate increases with time; and
- If $\beta = 1$, then the hazard rate is constant and the Weibull degenerates into the exponential case.

The reliability function (in Eq. (2.26)) against time is shown in Figure 2.12 for different values of β and α.

$$\boldsymbol{R_T(t) = exp(-\int_0^t h_T(x)dx) = \exp(-\int_0^t \frac{\beta}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1} dx) = \exp\left(-\frac{t}{\alpha}\right)^{\beta}}. \quad (2.26)$$

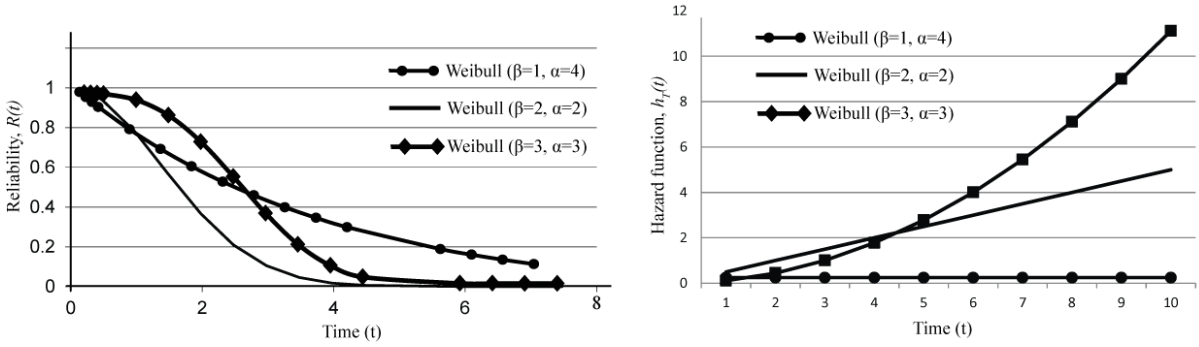


Figure 2.12: Hazard and reliability functions based on Weibull failure distribution.

A non-repairable 2-out-of-3 (2OO3) railway system with iid components will have hazard rate as

$$\boldsymbol{h_{2oo3}(t) = \frac{6\lambda \exp(-2\lambda t)(1-\exp(-\lambda t))}{3\exp(-2\lambda t)(1-\exp(-\lambda t)) + \exp(-3\lambda t)}}. \quad (2.27)$$

The term $3\exp(-2\lambda t)(1-\exp(-\lambda t)) + \exp(-3\lambda t)$ in the equation above is the reliability of the 2OO3 system. Hence, the mean time to failure (MTTF) is obtained by solving the following integral:

$$\boldsymbol{MTTF_{2oo3} = \int_0^{\infty} (3\exp(-2\lambda t)(1-\exp(-\lambda t)) + \exp(-3\lambda t))\, dt = \frac{5}{6\lambda}}. \quad (2.28)$$

The hazard rate as a function of time for the constant failure rate ($\lambda = 0.2$) is shown in Figure 2.13.

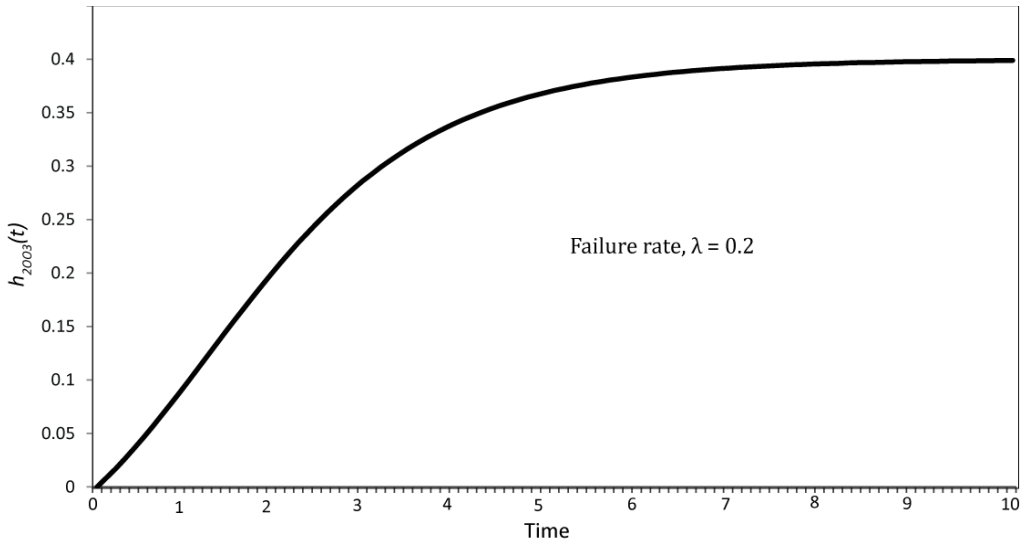


Figure 2.13: Hazard function for the 2-out- of-3 (independent and identically distributed) non-repairable system.

2.9.3 Monte Carlo (MC) Simulation

MC simulation, as an alternative to analytical calculation methods consists of many repetitions of a given sequence of calculations, each with randomly selected inputs (Rubinstein & Kroese, 2007; Kalos & Whitlock, 2004; Zio, 2009). The MC may be the only method for solving complex multi-dimensional stochastic modelling problems in reliability and availability engineering. The MC may be defined as a simulation method for obtaining approximate solutions to mathematical problems using random numbers. The basic principle underlying the MC simulation is explained in the following. Let $\mathbf{X} = [X_1, X_2, \dots, X_n]$ be a vector of random variables (or components in a system) with PDF $f(\mathbf{X})$ in some space Ω. If $g(\mathbf{X})$ is the limit state function representing the failure in the system then the failure event F can be written as $F = \{g(\mathbf{X}) \leq 0\}$. In other words, the probability of a failure event will be

$$\mathbf{Pr}(\boldsymbol{F}) = \mathbf{Pr}(\boldsymbol{g}(\boldsymbol{X}) \leq \mathbf{0})\,. \tag{2.29}$$

In the equation above, $\{g(\mathbf{X}) \leq 0\}$ corresponds to the failure domain Ω_F in the total sample space $\mathbf{X}$. Therefore, the $\Pr(F)$ is equivalent to the probability of $\mathbf{X}$ taking a value within the failure domain Ω_F. This is computed by integrating the $f(\mathbf{X})$ over the failure domain

$$\mathbf{Pr}(\boldsymbol{F}) = \int_{\boldsymbol{g(X)\leq 0}} \boldsymbol{f(X)dX} \ . \tag{2.30}$$

In the equation above, $f(\mathbf{X}) \geq 0$ and $\int_{\Omega} f(\mathbf{X})\mathrm{d}\boldsymbol{X} = 1$. In the case where Ω is a multi-dimensional space and $f(\mathbf{X})$ is a complicated function, then the computation of the $\Pr(F)$ through the integral above is not possible or feasible using analytic or numerical methods. By following the basis of simulation techniques, the definition of the failure probability above can be written as

$$\mathbf{Pr}(\boldsymbol{F}) = \int_{\boldsymbol{g(X)\leq 0}} \boldsymbol{f(X)dX} \ = \ \int \boldsymbol{I[g(X)\leq 0]f(X)dX} \, . \tag{2.31}$$

The *indicator function* $I[g(\mathbf{X}) \leq 0]$ takes the value 1 if the $g(\mathbf{X_i}) \leq 0$ otherwise it is equal to 0. Here $\mathbf{X_i}$ are samples drawn from the joint distribution of **X.** In other words, the integral problem in Eq. (2.30) can be written as an expected value of the *indicator function*

$$\mathbf{Pr}(\boldsymbol{F}) = \boldsymbol{E}[\ \boldsymbol{g(X)\leq 0}] \approx \frac{\mathbf{1}}{\boldsymbol{N}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} \boldsymbol{I[g(X)\leq 0]} \, . \tag{2.32}$$

In the equation above, N is the number of samples drawn (randomly) from the $f(\mathbf{X})$. In this way, we obtain an unbiased estimate with a standard deviation of the order $\sqrt{N}$.

For example, the well-known basic limit states function of the structural demand (S) and capacity (R) problem (Der Kiureghian, 2005; Bucher, 2009; Faber, 2012) is written as

$$\boldsymbol{g(R,S) = R - S}\,. \tag{2.33}$$

The probability of failure is calculated as

$$\mathbf{Pr}(\boldsymbol{F}) = \mathbf{Pr}(\boldsymbol{g(R,S)} \leq \mathbf{0}) = \mathbf{Pr}(\boldsymbol{R \leq S})\ . \tag{2.34}$$

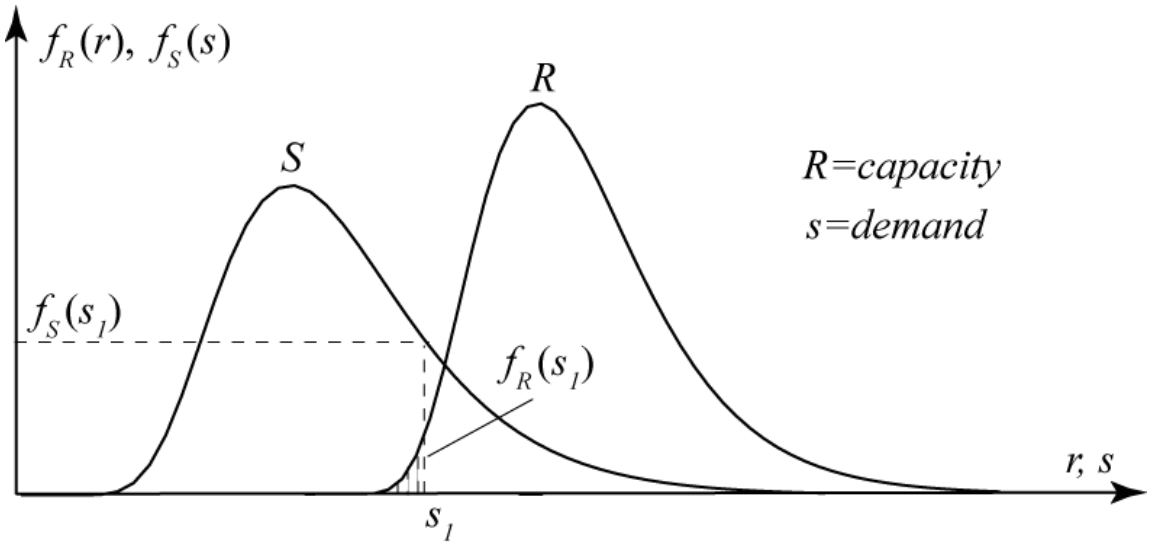


Figure 2.14: Illustration of the capacity and demand problem from the field of structural reliability.

The calculation of $\Pr(F)$ requires solving the 2-dimensional (corresponding to two random variables, R and S) integral. An analytical solution to the $g(R,S) = R - S$ problem above is obtained by transforming the 2-dimensional integral into a 1-dimensional integral. For a given value of demand $S = s_1$ the conditional probability of failure is written as $\Pr(F \mid S = s_1) = \Pr(R \leq s_1) = F_R(s_1)$. The graphical illustration of the problem is presented in Figure 2.14. The probability of failure is then obtained by using the total probability theorem:

$$\mathbf{Pr}(\boldsymbol{F}) = \int_{\boldsymbol{S}} \mathbf{Pr}(\boldsymbol{F} \mid \boldsymbol{S} = \boldsymbol{s_1}) \boldsymbol{f_S}(\boldsymbol{s})\, \boldsymbol{d}\, \boldsymbol{s} = \int_{\boldsymbol{S}} \boldsymbol{F_R}(\boldsymbol{s_1}) \boldsymbol{f_S}(\boldsymbol{s}) \boldsymbol{d}\, \boldsymbol{s}\,. \tag{2.35}$$

In the following, we solve the 2-dimensional integral problem above using MC simulation. Assume that capacity (KN/m^2) and demand (KN/m^2) follow a Normal distribution (see Figure 2.15) with parameter values $N{\sim}(\mu_R = 100.0\,, \sigma_R = 10.0)$ and $N{\sim}(\mu_S = 70.0, \sigma_S = 5.0)$, respectively and are uncorrelated. We generate $N = 30{,}000$ samples of R and S. Whether or not the individual sample falls into the failure domain is investigated. We estimate the $\Pr(R - S \leq 0)$ using the following indicator function

$$\mathbf{Pr}(\boldsymbol{F}) = \mathbf{Pr}(\boldsymbol{g}(\boldsymbol{R}, \boldsymbol{S}) \leq \mathbf{0}) \approx \frac{\mathbf{1}}{\boldsymbol{N}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} \boldsymbol{I}[\boldsymbol{r_i} - \boldsymbol{s_i} \leq \mathbf{0}]\,. \tag{2.36}$$

Only 113 samples fall into the failure domain out of the 30,000 samples. In this way, $\Pr(F) = \frac{113}{30{,}000} = 3.76 \cdot 10^{-03}$. The standard deviation $\sigma_{\Pr(F)}$ of the estimate can be determined from

$$\boldsymbol{\sigma}_{\mathbf{Pr}(\boldsymbol{F})} = \sqrt{\frac{\mathbf{Pr}(\boldsymbol{F})}{\boldsymbol{N}} - \frac{\mathbf{Pr}(\boldsymbol{F})^{\mathbf{2}}}{\boldsymbol{N}}} \approx \sqrt{\frac{\mathbf{Pr}(\boldsymbol{F})}{\boldsymbol{N}}} = \sqrt{\frac{\mathbf{3.76 \cdot 10^{-03}}}{\mathbf{30{,}000}}} = \mathbf{3.54 \cdot 10^{-04}}. \tag{2.37}$$

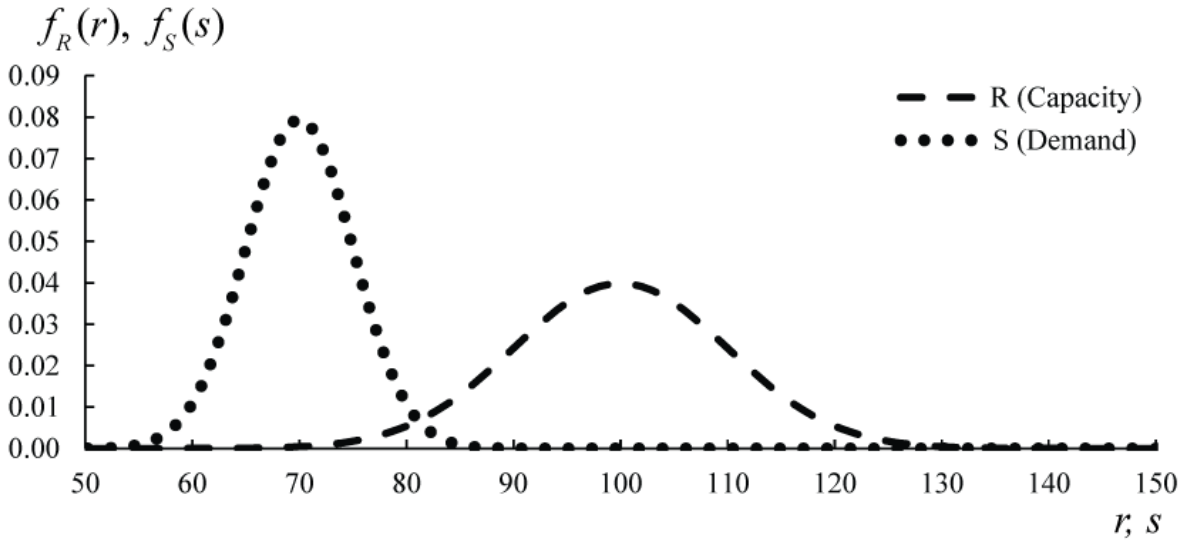


Figure 2.15: Normally distributed random variables corresponding to capacity (R) and demand (S).

It should be mentioned that the required number N of simulations is independent of the (integral) dimension of the problem. The problem with this simulation approach is that for small values of $\Pr(F)$ and small values of N the confidence of the estimate is very low.

The sampling process in MC simulation becomes difficult if the functional form of $f(\mathbf{X})$ is very complicated or Ω is high-dimensional. In that case, researchers use alternative sampling methods to sample from complicated distributions. FORM (First Order Reliability Method), SORM (Second Order Reliability Method), MCMC (Markov Chain Monte Carlo), rejection sampling and importance sampling are some of alternative methods (Kiureghian, 2005; Rubinstein & Kroese, 2007; Zio, 2013).

2.10 Summary

A large number of different techniques and tools can be utilized to analyse the risk and safety in railways. Some well-known methods, from the point of view of the railway application, are explained with the help of examples and the limitations of the presented methods are discussed. The fundamental problem with the different techniques and tools is that it is not clear that which technique and tool are more suitable for which situation and system as-

pect. The risk analysis process followed in the different techniques begins with different activities, finish with different activities and follow different ways and paths in between beginning and finish. Although every technique and tool are based on different analysis and evaluation criteria; however, these techniques and tools can be suitable to compare and to classify safety and risk problems of different railway systems. Qualitative and semi-quantitative techniques like risk matrix and FMEA compare and classify system safety and risks mainly based on experience of system experts. Different experts may use different or even totally opposite ways of modelling the same system (behavior and characteristics) in qualitative analysis.

Quantitative techniques such as Fault Tree, Event Tree, Markov Model, hazard functions and Monte Carlo simulation techniques evaluate railway risk and safety based on calculation results using mathematical models. It is only the quantitative technique, which provides a mean to compute the parameters related to risk and safety problems. However, the parameters of the mathematical models themselves can be highly uncertain.

In conclusion, it can be seen that all methods are not well suited to all kinds of risk and safety problems, but some are more useful than others (Rouvroye & van den Bliek, 2002; Braband, 2001). Therefore, care must be taken in the selection of a risk analysis method and decisions need to be taken on a case-by-case basis. For example, there can be a case when one analysis technique (say Fault Tree Analysis) is not enough and one needs to use a combination of techniques (say Monte Carlo simulation and Fault Tree Analysis or FMEA and Fault Tree Analysis.)

CHAPTER 3: INTRODUCTION TO BAYESIAN NETWORKS

This section describes Bayesian Networks, which use a graph-based representation to model joint distributions of random variables in a compact way. Here, sufficient introduction to Bayesian Networks is provided so that methods and models presented in the coming chapters can be better understood. For readings on Bayesian Networks and associated topics in detail, readers are referred to (Jensen & Nielsen, 2007; Koller & Friedman, 2009; Ahmed, 2010; Murphy, 2002). For the application of Bayesian Networks to risk assessment and decision support we refer to (Bensi, 2010; Hanea & Ale, 2009(b); Heredia-Zavoni, et al., 2012; Spackova & Straub, 2013; Straub, 2009).

3.1 Terminology in Bayesian Networks

Bayesian Networks are directed acyclic probabilistic graphical models that represent joint probability distribution of all variables in the network. They consist of a set of nodes (ellipse), which correspond to discrete or continuous random variables in Bayesian Networks and a set of directed links (arrows), which represent (probabilistic) dependence structure among nodes in Bayesian Networks. Consider the Bayesian Networks shown in Figure 3.1 which models dependencies among six random variables $\mathbf{X} = [X_1, \dots, X_6]$. For example, the random variable X_5 is probabilistically dependent on the variables X_3, X_2 and X_4. In Bayesian Networks the nodes X_3, X_4, X_5 are the children of X_2, which is parent of the formers. The variables X_1 and X_2 have no parents and the variables X_5 and X_6 have no children. If the Bayesian Networks consist of discrete random variables then each node will have a set of mutually exclusive and collective exhaustive states. A conditional probability table (CPT) is attached to child random variables. The CPT is utilized to describe the conditional probability mass function of a discrete random variable, given each of the mutually exclusive states

of its parents. The CPT specifies how strongly the dependent nodes influence each other. A node with no parents will have marginal or unconditional probability table, called prior probability.

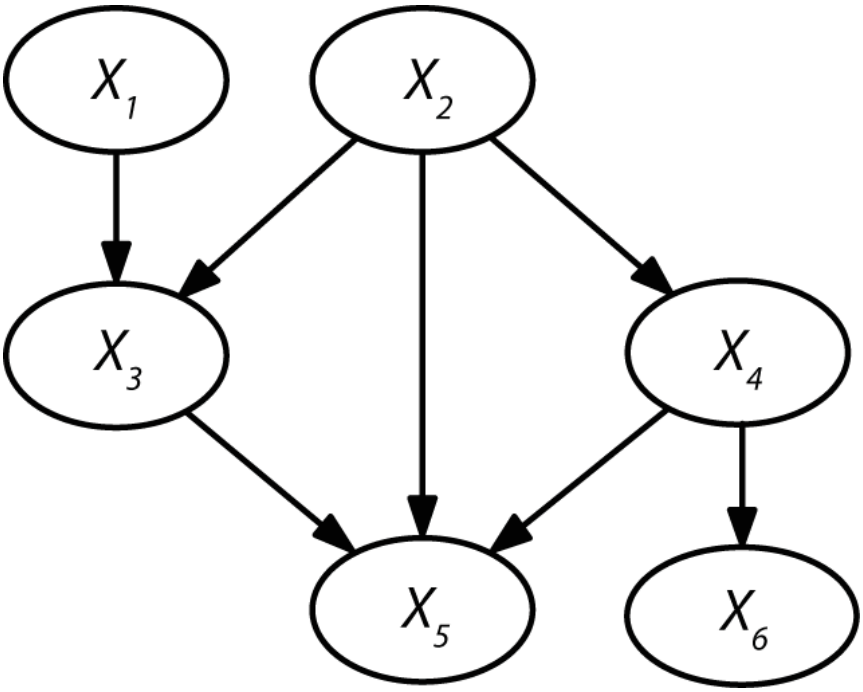


Figure 3.1: A sample Bayesian Network

3.2 Construction of Bayesian Networks

Modelling and analysis of system safety using Bayesian Networks require the complete understanding of the safety problem and its influencing factors (nodes in Bayesian Networks). The construction of Bayesian Networks requires graphical and numerical tasks (Kjaerulff & Madsen, 2007). The graphical task includes the definition of the graphical model in terms of its nodes and dependencies (causal relations). For example, a graphical model, its nodes and dependence structure is shown in Figure 3.1.

The conditional relations among influencing factors must be developed in a way that the d-separation properties, which will be explained in next Section, of the model are satisfied. The numerical task includes the construction of the CPTs to define the joint distribution over all random variables in Bayesian Networks. The CPTs are also based on dependence relations between the nodes and their joint distribution can be based on empirical investigation, theoretical models, expert and factual judgments, or combinations of all. For example, the PMF and the joint distributions of all the nodes of the sample Bayesian Networks above are shown in Figure 3.2 and Figure 3.3. For simplicity, each node is assigned only two states. (''+'' and ''-'' correspond to occurrence and non-occurrence states of each random variable, respectively.)

$P(X_1)$	
+	0.1
-	0.9

$P(X_4 \mid X_2)$		
X_2	+	-
+	0.6	0.2
-	0.4	0.8

$P(X_3 \mid X_2, X_1)$				
X_2	+		-	
X_1	+	-	+	-
+	0.9	0.6	0.5	0.05
-	0.1	0.4	0.5	0.95

$P(X_6 \mid X_4)$		
X_4	+	-
+	0.75	0.1
-	0.25	0.9

$P(X_2)$	
+	0.15
-	0.85

Figure 3.2: (Conditional) Probability tables for $X_1, \dots, X_4$.

$P(X_5 \mid X_2, X_3, X_4)$								
X_2	+				-			
X_3	+		-		+		-	
X_4	+	-	+	-	+	-	+	-
+	0.9	0.6	0.35	0.2	0.3	0.05	0.01	0
−	0.1	0.4	0.65	0.8	0.7	0.95	0.99	1

Figure 3.3: Conditional probability table for X_5.

3.3 Conditional independence in Bayesian Networks

The concept of conditional independence, so-called ‘’d-separation’’ (or blocked) properties is important when using Bayesian Networks. The conditional independence strongly reduces computational and modelling efforts. How each node is conditionally independent of its non-descendants given its predecessors, called its parents, is explained below. Consider three types of connections (see Figure 3.4) in the sample Bayesian Networks above. A serial connection is formed by X_2, X_4, X_6. In this connection, the evidence is transmitted through the network if the state of the intermediate random variable X_4 is not known with certainty. A serial connection is d-separated once the intermediate random variable X_4 is instantiated, which blocks the information path between X_2 and X_6. A diverging connection is formed by X_4, X_5, X_6. In this connection, the evidence is transmitted when the state of the common parent variable X_4 is not known with certainty. In a converging connection like X_1, X_2, X_3 the evidence is transmitted only if there is some information about the common child variable X_3 or (one of) its descendant, which is X_5 in the Bayesian Networks. In other words, a converging connection is d-separated (blocked) when there is no evidence on the random variable X_3.

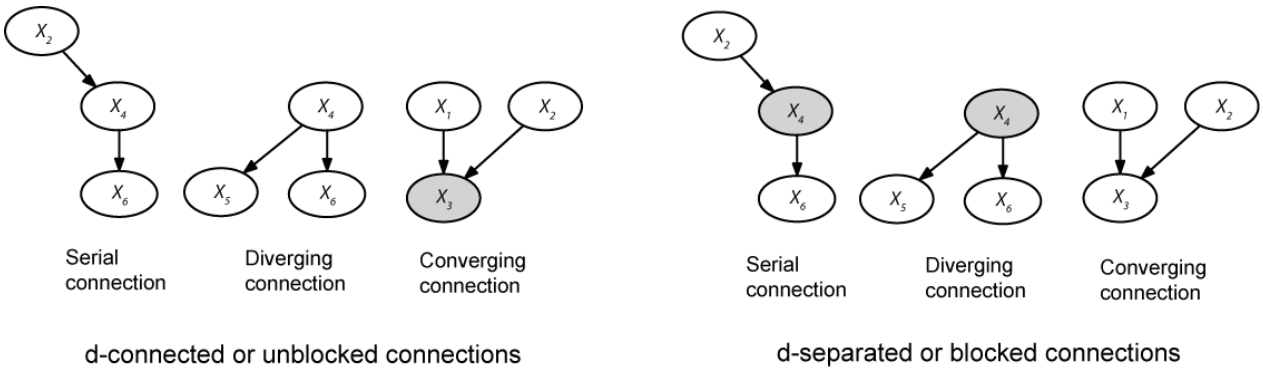


Figure 3.4: A graphical representation of d-separation properties of Bayesian Networks connections.

3.4 Joint probability distribution in Bayesian Networks

Bayesian Networks give a complete representation of the full joint probability tion $p(\mathbf{x})$ of all the variables in a network. For example, consider the network in Figure 3.1 with random variables, $\mathbf{X} = [X_1, \dots, X_6]$, which has finite set of mutually exclusive and collective exhaustive states. Based on conditional independence and chain rule[2], the Joint PMF of all random variables **X** is written as the product of the conditional PMFs

$$\boldsymbol{p(\mathbf{x}) = p(x_6 \mid x_4)p(x_5 \mid x_4, x_3, x_2)p(x_4 \mid x_2)p(x_3 \mid x_2, x_1)p(x_2)p(x_1)}\,. \qquad (3.1)$$

In the equation above, the joint distribution is factored into the product of local conditional PMFs. This factorization is useful for quantified analysis of Bayesian Networks. This Joint PMF can be generalized as

[2] $p(\mathbf{x}) = p(x_1, \dots, x_2) = p(x_1 \mid x_2, \dots, x_n)p(x_2 \mid x_3, \dots, x_n), \dots, p(x_{n-1} \mid x_n)p(x_n)$

$$\boldsymbol{p}(\mathbf{x}) = \boldsymbol{p}(\boldsymbol{x_1}, \ldots, \boldsymbol{x_6}) = \prod_{\boldsymbol{i=1}}^{\boldsymbol{6}} \boldsymbol{p}(\boldsymbol{x_i} \mid \mathbf{pa}(\boldsymbol{x_i}) \,. \tag{3.2}$$

In the generalized form above, $\mathrm{pa}(x_i)$ is the set of parents of random variables X_i. Bayesian Networks have advantages that they can perform tasks related to state (1) prediction (forward analysis) using total probability theorem and (2) estimation or diagnostic (backward analysis) using Bayes' rule.

3.5 Probabilistic Inference in Bayesian Networks

By making use of Bayesian Networks one can perform three tasks – structural learning (SL), parameter learning (PL), and probabilistic inference (PI). SL and PL are data driven processes. In SL, algorithms determine the topology of the model like number of arrows and their directions in Bayesian Networks. In PL, unknown parameters of the joint or conditional distributions in Bayesian Networks are determined from data using algorithms like Expectation Maximization (EM) algorithm. For more details on SL and PL we refer to (Jensen & Nielsen, 2007; Koller & Friedman, 2009; Russel & Norvig, 2010). PI is used to compute the probability distributions for a set of variables, given some evidence. In this work, Bayesian Networks are used only for PI.

A number of questions related to probability of (set of) variables in Bayesian Networks can be answered using PI. Consider the network in Figure 3.1 where all random variables have $m = 2$ states. (+ and – represent the occurrence and nonoccurrence states of the binary random variables in the Bayesian Networks, respectively.) Mainly, we answer questions like: what is the probability (of a set) of random variables X_6 being in a specific state, say +, given that another (set of) random variables X_3 is observed to be equal to +: $p(X_6 \mid X_3) = ?$ This question can be answered by following conditional probability,

$$\boldsymbol{p}(\boldsymbol{X_6} \mid \boldsymbol{X_3}) = \frac{\boldsymbol{p}(\{\boldsymbol{X_6} = +\} \cap \{\boldsymbol{X_3} = +\})}{\sum_{\boldsymbol{X_6}} \boldsymbol{p}(\{\boldsymbol{X_6} = +\} \cap \{\boldsymbol{X_3} = +\})} = \frac{\boldsymbol{p}(\boldsymbol{X_6}, \boldsymbol{X_3})}{\boldsymbol{p}(\boldsymbol{X_3})} \quad . \tag{3.3}$$

We solve the joint PMFs (numerator) and marginalized probability (denominator) in the equation above. A number of exact and approximate algorithms exist to answer probability questions in Bayesian Networks. The exact inference methods such as inference by enumeration and variable elimination (see below) are used for small and simpler Bayesian Networks, which have discrete random variables.

3.6 Probabilistic inference by enumeration

Consider the joint distribution $p(X_6,\ X_3)$ in Eq. 3.4 where the non-query variables for this query are X_1, X_2, X_4, X_5. To get joint PMF we enumerate possible values of variables in Eq. (3.1):

$$\boldsymbol{p}(\boldsymbol{X_6}, \boldsymbol{X_3}) = \sum_{\boldsymbol{X_1}, \boldsymbol{X_2}, \boldsymbol{X_4}, \boldsymbol{X_5}} \boldsymbol{p}(\boldsymbol{x_6} \mid \boldsymbol{x_4}) \boldsymbol{p}(\boldsymbol{x_5} \mid \boldsymbol{x_4}, \boldsymbol{x_3}, \boldsymbol{x_2}) \boldsymbol{p}(\boldsymbol{x_4} \mid \boldsymbol{x_2}) \boldsymbol{p}(\boldsymbol{x_3} \mid \boldsymbol{x_2}, \boldsymbol{x_1}) \cdot \cdot \boldsymbol{p}(\boldsymbol{x_2}) \boldsymbol{p}(\boldsymbol{x_1}). \tag{3.4}$$

Above equation tells that product of all terms in Eq. (3.1) should be summed up over X_1, X_2, X_4, X_5. If the product of Eq. (3.4) is $f(X_1, X_2, X_4, X_5)$ then whole answer of $p(X_6, X_3)$ is the sum of m^n (n = number of variables, m= number of states of random variables) equations. As we have four variables each having two states; therefore, we need to add solutions of sixteen equations:

$$\boldsymbol{p}(\boldsymbol{X_6}, \boldsymbol{X_3}) = \boldsymbol{f}(\boldsymbol{X_1}, \boldsymbol{X_2}, \boldsymbol{X_4}, \boldsymbol{X_5}) + \boldsymbol{f}(\overline{\boldsymbol{X_1}}, \boldsymbol{X_2}, \boldsymbol{X_4}, \boldsymbol{X_5}) + \cdots + \boldsymbol{f}(\overline{\boldsymbol{X_1}}, \overline{\boldsymbol{X_2}}, \overline{\boldsymbol{X_4}}, \overline{\boldsymbol{X_5}}) \,. \tag{3.5}$$

In equation above, each product, say $f(\overline{X_1}, X_2, X_4, X_5)$ represents one solution of enumeration. Similarly, for marginalized probability $p(\mathbf{x_3})$ in Eq. (3.3) we enumerate possible values of variables in Eq. (3.1):

$$\boldsymbol{p(X_3)} = \sum_{\boldsymbol{X_1, X_2, X_4, X_5, X_6}} \boldsymbol{p(x_6 \mid x_4) p(x_5 \mid x_4, x_3, x_2) p(x_4 \mid x_2) p(x_3 \mid x_2, x_1)} \cdot \\ \cdot \boldsymbol{p(x_2) p(x_1)}. \tag{3.6}$$

We need to solve $\mathbf{2^5 = 32}$ equations that correspond to five (non-query) variables for $\boldsymbol{p(X_3)}$. Finally, using probabilities from Figure 3.2 and Figure 3.3, we get $p(X_6 \mid X_3) \approx (0.3701, 0.6298)$. It implies that this inference technique will become ineffective when the Bayesian Networks have (1) large variables and/or (2) large states of the variables. For example, Bayesian Networks with 20 random variables, each having two states will require $2^{20} = 1{,}048{,}576$ enumeration.

3.7 Probabilistic inference by variable elimination

The variable elimination algorithm involves three steps: (1) pulls out terms form the joint probability distributions of Bayesian Networks by exploiting the use of d-separation properties (2) combine together parts of Bayesian Networks to obtain smaller Bayesian Networks with larger terms, i.e. joint PMFs and (3) enumerate over these smaller parts of Bayesian Networks. These operations continue until we achieve a desired distribution. In other words, it is a way to determine the distribution of a subset of variables in Bayesian Networks by continuously eliminating the nodes from the Bayesian Networks that are independent of the subset of interest. For example, consider the Bayesian Networks in Figure 3.1 where it is required to compute marginalized probability $p(\mathbf{x_6})$. By following Eq. (3.4), $p(\mathbf{x_6})$ can be written as

$$\boldsymbol{p(X_6)} = \sum_{X_1,X_2,X_3,X_4,X_5} \boldsymbol{p(x_6 \mid x_4)p(x_5 \mid x_4,x_3,x_2)p(x_4 \mid x_2)p(x_3 \mid x_2,x_1)} \cdot \\ \cdot \boldsymbol{p(x_2)p(x_1)}. \tag{3.7}$$

As mentioned earlier, this require the computation and summation of the $2^5 = 32$ equations. However, variable elimination method will reduce this computational effort by exploiting the use of statistical independencies in Bayesian Networks and summing the joint distribution of the variables over all states of the variables, which need to be eliminated. Mathematical interpretation of the variable elimination is presented below. By making use of the distributive law, we can rewrite the Eq. (3.7)

$$\boldsymbol{p(X_6)} = \sum_{X_1} \boldsymbol{p(x_1)} \sum_{X_2} \boldsymbol{p(x_2)} \sum_{X_3} \boldsymbol{p(x_3 \mid x_2,x_1)} \sum_{X_4} \boldsymbol{p(x_6 \mid x_4)p(x_4 \mid x_2)} \cdot \\ \cdot \sum_{X_5} \boldsymbol{p(x_5 \mid x_4,x_3,x_2)}. \tag{3.8}$$

We make use of the d-separation properties and observe that $\sum_{X_5} p(x_5 \mid x_4,x_3,x_2) = 1$, $\sum_{X_3} p(x_3 \mid x_2,x_1) = 1$, and $\sum_{X_1} p(x_1) = 1$. However, the terms $\sum_{X_2} p(x_2)$ and $\sum_{X_4} p(x_6 \mid x_4)p(x_4 \mid x_2)$ remain unchanged, since X_6 is a child of X_4 and descendent of X_2. The resulting joint probability distribution is given below and its corresponding Bayesian Networks is shown in Figure 3.5(B).

$$\boldsymbol{p(X_6)} = \sum_{X_2,X_4} \boldsymbol{p(x_6 \mid x_4)p(x_4 \mid x_2)p(x_2)} \tag{3.9}$$

We can observe that this term has become computationally efficient as the largest number of probability values that must be handled at any time is reduced to $2^3 = 8$.

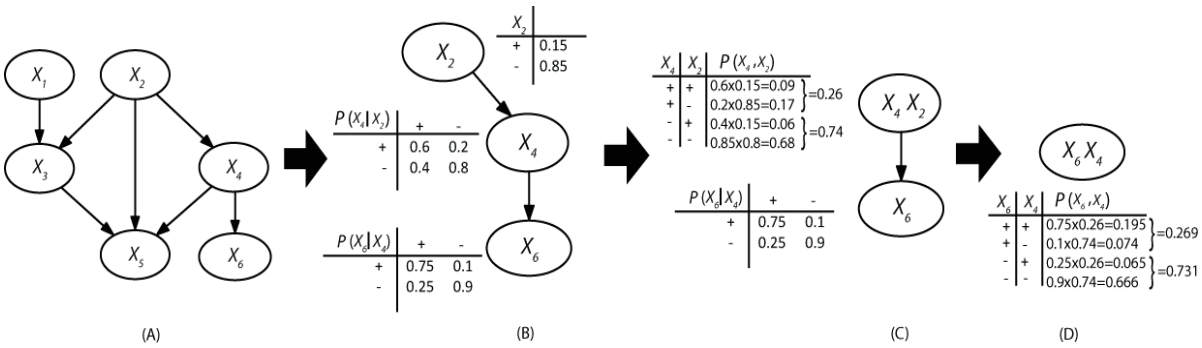


Figure 3.5: Bayesian Networks framework obtained during probabilistic inference by variable elimination.

Next step is to combine together parts of larger Bayesian Networks to obtain smaller Bayesian Networks, but with large terms. For example, Bayesian Networks in Figure 3.5 (C) is obtained by joining together parts of Bayesian Networks in Figure 3.5 (B). We obtain smaller Bayesian Networks with a large term $p(X_4, X_2)$. The same operation is carried to obtain large term $p(X_6, X_4)$ in Figure 3.5 (D). Final step is to marginalizing out variables like X_2 and X_4 from large terms. For example, marginalizing out X_2 from $p(X_4, X_2)$ will give us $p(+X_4, -X_4) = (0.26, 0.74)$. The graphical representation of these operations is shown in Figure 3.5 for $p\ (x_6)$ where we obtain $p(+x_6, -x_6) = (0.269, 0.731)$. The variable elimination algorithm for Joint PMF of $p\ (x_6)$ followed a specific order of elimination operations; first X_5, second X_3, third X_1, and at last X_4. When performing variable elimination, given there are evidences on some variables in Bayesian Networks, we sum over all variables except the evidence variables.

The order of elimination determines the number of maximum probability values (or computational complexity) that need to handle at any time. The most optimal order is the one that pushes the summation operations as far right as possible.

3.8 Approximate inference for Bayesian Networks

Simple Bayesian Networks can be evaluated without the use of computers, using exact inference algorithms. However, large and complex Bayesian Networks require the aid of computers. In general, the computational efforts (in terms of time and space) increase with

the increase in random variables and their states in Bayesian Networks. In this case, the exact inference algorithms will become ineffective and we make use of approximate algorithms like direct sampling, rejection sampling, likelihood weighting and Markov Chain Monte Carlo (MCMC) that are based on simulation. The approximate algorithms have the advantage that they allow treatment of continuous random variables. So, discretization of continuous variables can be avoided. However, the main disadvantage of the approximate algorithms is that it is difficult to assess their accuracy. Therefore, the results based on the approximate algorithms cannot be relied upon. For details on approximate algorithms, readers are referred to (Koller & Friedman, 2009; Russell & Norvig, 2010). A number of exact and approximate algorithms are implemented in software, which are useful for a large number of engineering problems.

3.9 Dynamic Bayesian Networks

Bayesian Networks with repetitions over time are called Dynamic Bayesian Networks. The Dynamic Bayesian Networks will be called homogenous if the repetitions are identical in all time steps. Each time step (or slice) has a Bayesian Networks model that will evolve over time; consequently the joint distribution of the Bayesian Networks will change. There will be links within each time slice and from one to the next one. Time dependence between different random variables is managed by connecting the variables with directed links and by defining the transition probabilities between the states of the variables at that time. For example, in the Dynamic Bayesian Networks shown in Figure 3.6, there is a link from X to Y (where X and Y constitute a complete BN model in one time slice) and from X_1 to X_2 and X_3. In a homogeneous and discrete Dynamic Bayesian Networks, the conditional PMF of the random variables and the model structure are identical in all time slices.

The Dynamic Bayesian Networks is based on Markov assumption; for given system state at time t, the state at $t+1$ is statistically independent of the state at $t-1$: $p(x_{t+1} \mid x_t, x_{t-1}, \dots, x_1) = p(x_{t+1} \mid x_t)$. In dynamic problems, great care is required to check whether the Markov assumption holds or not. In the Dynamic Bayesian Networks shown in Figure 3.6, this Markov assumption does not hold because random variable e.g. X_4 requires knowledge on X_2 together with X_3. Thus, the random variable X_4 is not

independent of X_2 given X_3. For compact visualization of the Dynamic Bayesian Networks model in Figure 3.6, alternatively it is possible to show only one time slice and to introduce links from one time slice to the next with a number indicating the order of the time slice. For example, concise representation of the Dynamic Bayesian Networks shown in Figure 3.6 can be seen in Figure 3.7. In other words, the Dynamic Bayesian Networks is a compact representation for encoding structured distribution over time. For further details on Dynamic Bayesian Networks we refer to (Murphy, 2002; Jensen & Nielsen, 2007).

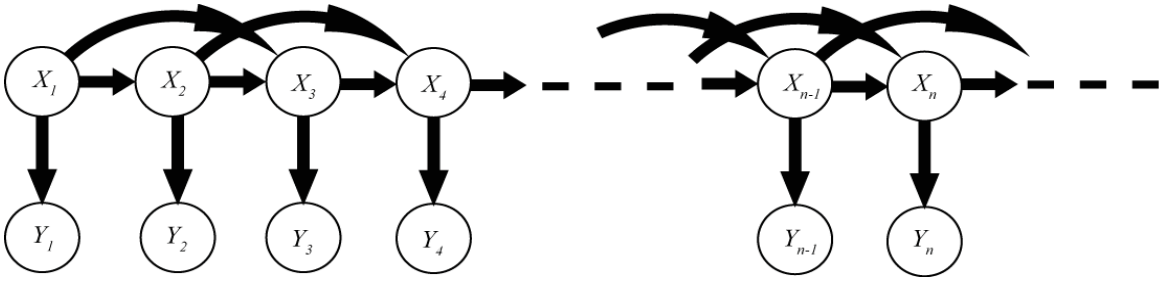


Figure 3.6: Schematic representations of a Dynamic Bayesian Network model (DBN).

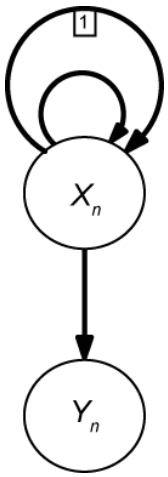


Figure 3.7: A concise representation of dynamic Bayesian Network.

3.10 Influence diagrams (IDs)

IDs are extensions of Bayesian Networks. A sample IDs is shown in Figure 3.8. In the IDs, additional nodes for decisions (rectangles) and utilities (diamond shape) are attached to the Bayesian Networks. The directed links (arrows) represent probabilistic dependencies among the system variables (represented by X), decision variables (represented by a) and utility variables (represented by U) in the network.

A decision analysis with given information (on system states, decision alternative and their utility functions) is called prior analysis. In the IDs with given information, the decision nodes are introduced as parents to the system variables and the utility nodes. In other words, the decision nodes influence both the system and utility nodes. For example, the decision optimization problem in Figure 3.8 is a simple representation of a prior decision analysis using IDs. In the prior analysis, the evaluation is made on the basis of probabilistic modelling and statistical values available prior to any decision.

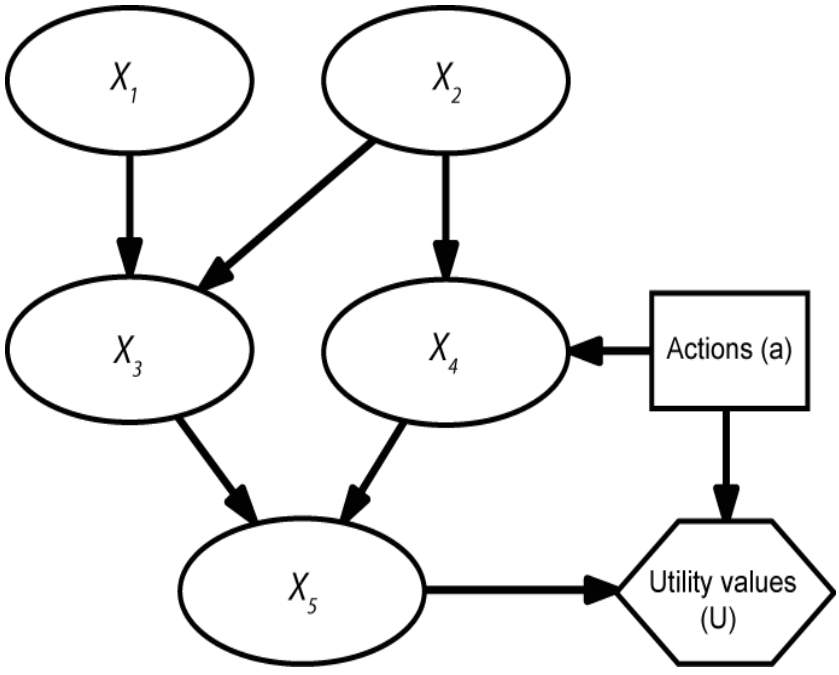


Figure 3.8: A sample influence diagram for prior analysis.

The optimal decision $\mathbf{a_o}$ is identified as the decision with minimal expected costs, which is equivalent to the maximized expected utility,

$$\mathbf{a_o} = \mathbf{arg}\max_{\mathbf{a}} \mathbf{E}[\mathbf{U}(\mathbf{a},\mathbf{x})] \tag{3.10}$$

$$= \mathbf{arg}\max_{\mathbf{a}} \sum_{\mathbf{x}} \boldsymbol{U}(\mathbf{a},\mathbf{x}) \cdot \boldsymbol{p}(\mathbf{x} \mid \mathbf{a}). \tag{3.11}$$

In equations above, $\mathbf{a} = (\mathrm{a}_1, \mathrm{a}_2, .., \mathrm{a}_n)^T$ are decision alternatives, $U(.)$ is the utility, $p(.)$ is the probability, E[.] is the expectation operator and $\mathbf{x}$ is a vector of system variables (from Bayesian Networks) that influence different decision alternatives. In prior analysis, the simple comparison of utilities associated with different system outcomes (that are influenced by decisions) can be performed, and the decision alternatives can be ranked and optimized.

There are few applications of Bayesian Networks to the railways. For example, (Marsh & Bearfield, 2007) use Bayesian Networks for the representation of a parameterized FTA for SPAD; (Oukhellou, et al., 2008) develops Bayesian Networks model for identifying and classifying rail defects based on sensor data; (Mahboob, et al., 2012(a)) quantifies hazards in railway signalling; (Lu, et al., 2011) proposed a Bayesian Networks approach to model causal relationships among risk factors for subway systems. However, no studies exist on how to model risk and reliability in complex railways – characterized by a number of advanced aspects, which are explained in section 5. Furthermore, the computation of the IMs for complex railway systems using Bayesian Networks has not been discussed so far. For application of Bayesian Networks to different industries, we refer to (Straub & Kiureghian, 2010; Darwiche, 2010; Mohaghegh, et al., 2009; Holicky & Diamantidis, 2008; Lampis & Andrews, 2009) and the references therein.

CHAPTER 4: RISK ACCEPTANCE CRITERIA AND SAFETY TARGETS

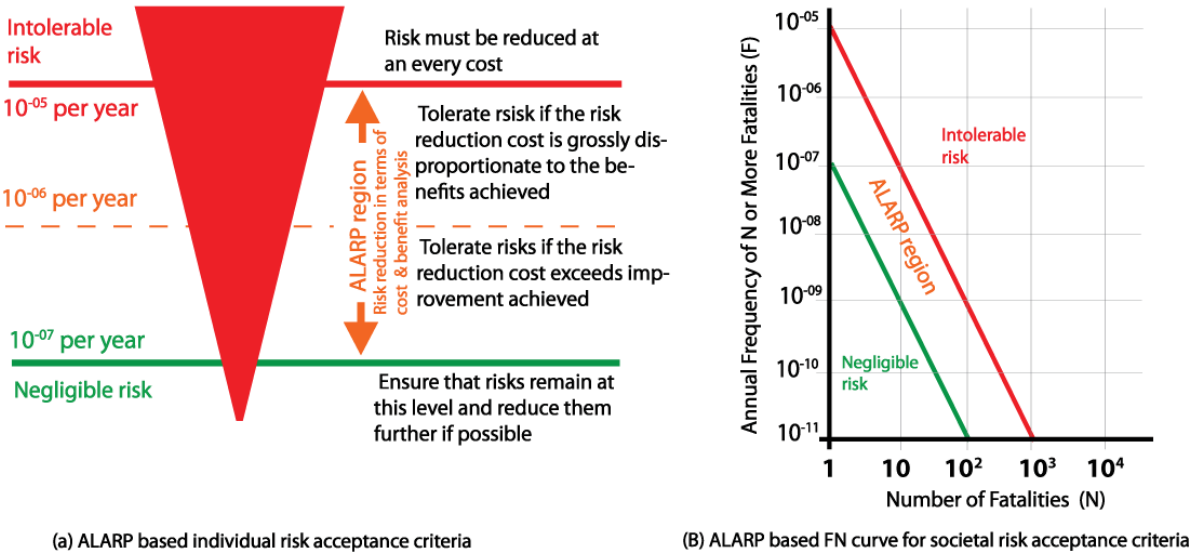
4.1 Introduction

Railways are subject to different hazards, which can lead to life safety risks. It is not possible to completely eliminate hazards in engineering systems, including railways. Therefore, the real objective must always be to identify, quantify, reduce (if necessary) and control the risks. Risks on the railways are determined regularly to investigate the effects of new solutions related to technology and regulations, introduced periodically to improve the performance and safety of the system. These risks are compared against target values to determine their level of presence and acceptance. Risk acceptance criteria are given, for example, in the form of two extreme limits on the annual probability of an accident depending on the consequence of the accident in terms of fatalities. In the case of fatalities, the classical way of representing risk arising from a railway system is the individual risk, expressed in terms of an annual fatality rate for a person who is exposed to the given situation at a given point in time; and the societal risks, expressed through a plot of the frequency of the number of fatalities (F) against the number of fatalities (N), the so-called FN curve, see Figure 4.1. The acceptance of risks becomes more rigid as the number of fatalities increases in societal risk acceptance criteria. A number of risk acceptance criteria exist for engineering systems that are also used for railways.

4.2 ALARP (As Low As Reasonably Possible) criteria

The ALARP is widely accepted as *''best practice''* in the railway (Beugin, et al., 2007; Braband, et al., 2006). ALARP provides several variations between the two extremes. According to the ALARP approach, a tolerable region exists between the regions of intolerable and negligible risks (see Figure 4.1). In the tolerable region, risk reduction is desirable and

is undertaken only if some benefit (evaluated using BCA, utility values and WTP) is obtained. The risk must be made ALARP in the tolerable region. It should be mentioned that the two extremes in the ALARP criteria are system and goal specific. In other words, two similar railway systems that are located in different socio-economic and operational conditions can have different risk acceptance criteria. The criterion line in the ALARP based FN curve is dependent on the number of people exposed to a hazard caused by any failure. This criterion line can move up or down depending on the change in the number of people in danger.



(a) ALARP based individual risk acceptance criteria

(B) ALARP based FN curve for societal risk acceptance criteria

Figure 4.1: An ALARP based individual and collective risk acceptance criteria.

4.3 MEM (Minimum Endogenous Mortality) criterion

MEM risk acceptance criteria, shown in Figure 4.2, are also utilized in the railway (Kerbs, et al., 2000). According to the MEM principle, the individual (age-dependent) risk due to a particular technical system must not exceed, for example, $1/20^{th}$ or 5% of the MEM (e.g. for the age group between 5 and 15 years it is given as $2E-04$ per person and year). (Here $1/20^{th}$ considers that an individual is using 20 technical systems in his or her daily life and

each technical system causes same level of life safety risk.) Thus, the (5 to 15 years age-specific) individual risk acceptance level becomes $\frac{1}{20} \cdot 2E-04 \quad = 1E-05$ per person and year. The acceptance of risks becomes more rigid as the number of fatalities increase.

In the ALARP and MEM criteria above, intolerable risk limits exists. If the risks cross this intolerable limit, then one must adopt safety measures – regardless of cost – to bring the risks into the tolerable region. One may require some socio-economic considerations (such as CBA, WTP, LQI and other utility based methods) in making decisions on safety measures when the risks are already in the tolerable region (e.g. the ALARP region).

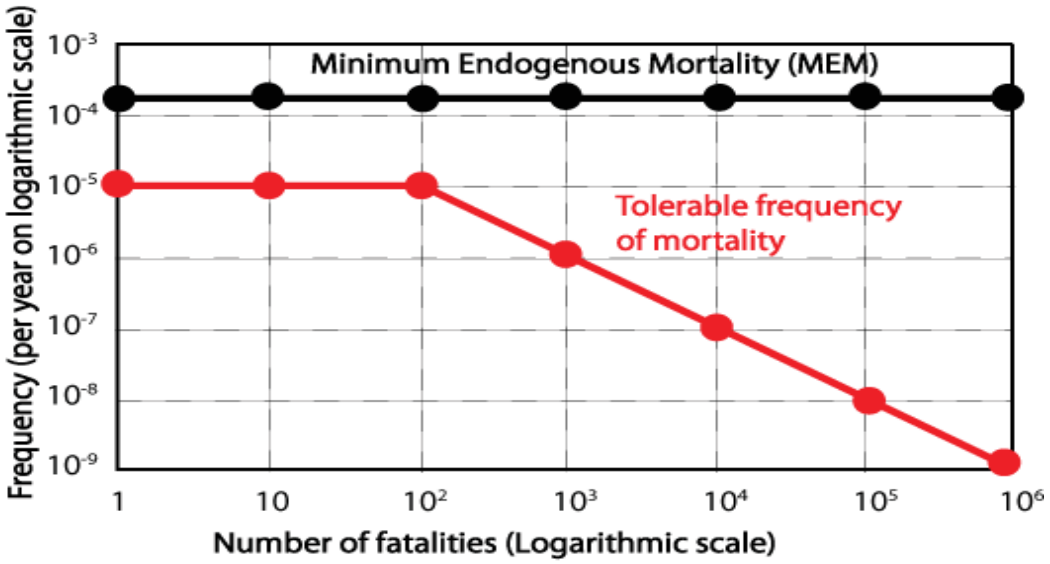


Figure 4.2: The Minimum Endogenous Mortality based criteria for risk acceptance.

4.4 MGS (Mindestens Gleiche Sicherheit) criteria

This criterion is well explained in Article 2(2) of the German Railway Building and Operation Regulations, called EBO: exceptions to the accepted rules of engineering practices may

be made if at least the same level of safety is demonstrated which would be achieved by compliance with these rules.

The MGS criterion requires that any new technology should be designed in such a way that on a global level it must offer at least the same level of risk as the technology used in the past. Complete understanding of both new and old engineering systems, together with their operational conditions, is required in order to implement the MGS criteria.

4.5 Safety Integrity Levels (SILs)

The exact quantification of systematic (such as human) error is not possible; however, random failures can be quantified more precisely. The idea behind the SIL concept is to create a balance between the measures for preventing systematic errors and random failures. The concept of SIL is a way to measure the performance of a safety function for a safety technology. It is a concept of discrete levels of safety requirements for safety functions, subsystems or components. An SIL concept involves two factors:

- A range of values for a rate of failures in the high/low demand mode of operation; and
- Measures adopted (during the design phase of the system).

SIL	High-demand mode of operation (Probability of dangerous failures per hour)	Low-demand mode of operation (Probability of dangerous failures per hour)
SIL 4	$10^{-9} \leq THR < 10^{-8}$	$THR < 10^{-7}$
SIL 3	$10^{-8} \leq THR < 10^{-7}$	$10^{-7} \leq THR < 10^{-6}$
SIL 2	$10^{-7} \leq THR < 10^{-6}$	$10^{-6} \leq THR < 10^{-5}$
SIL 1	$10^{-6} \leq THR < 10^{-5}$	$10^{-5} \leq THR < 10^{-4}$

Figure 4.3: A definition of safety integrity levels (SILs).

The SIL definitions in Figure 4.3 are adopted from EN 50128 (Railway applications: software for railway control and application), EN 50129 (Railway applications: safety related electronic systems for signalling), IEC 61508 (Functional safety of electrical/electronic/programmable systems) and CENELEC (European Committee for Electrotechnical Standardization) standards (IEC 61508, 2000; CENELEC, 2012). Level 4 and level 1 correspond to the highest and lowest safety requirements, respectively. An SIL can be assigned to the safety relevant functions of a sub-system or component of a system. We apply the SIL concept in the identification of the safety requirements for a PSD system and its safety functions, see Chapter 6.

4.6 Importance Measures (IMs)

The idea of IMs was first introduced by Birnbaum (Birnbaum, 1969). It is based on the fact that, usually, not all components contribute to system risk, safety and reliability in the same way, but some components are relatively more important than others. Therefore, the components with higher importance should be treated carefully in the design, maintenance and operation phases of a system. The IMs can be used to rank the components of a system according to their importance. There are two classes of IM, based on structural and reliability importance. The structural importance measure (SIM) considers the importance of a component due to its position in the system and is not concerned about its reliability. So, SIM cannot classify the components that occupy similar structural positions but have different reliabilities. The reliability importance measure (RIM) not only considers the position of the component in the system but the reliability of the component also.

A number of IMs exist that can be used to rank important components (Birnbaum, 1969; Fussell, 1975; Borgonovo, et al., 2003; Borgonovo & Apostolakis, 2001). For instance, FV and RAW are commonly used IMs in the nuclear industry (U.S.N.R.C, 2012; Kang, et al., 2002). RAW identifies the increase in the system risks if a particular component failure in the system has occurred. The FV gives the fractional contribution of a component failure towards the system failure. The increase in the occurrence probability of the component failure will lead to the increase in the FV value. For instance, the NRC regulatory guide 1.174 suggests an FV of 0.05 at the system level and 0.005 at the component level for nu-

clear systems (U.S.N.R.C, 2012). Another study suggests the following criteria for importance analysis of in-service testing for low safety significant components (LSSC), intermediate safety significant components (ISSC) and high safety significant components (HSSC) in the nuclear industry (Kang, et al., 2002):

- LSSC: FV<0.005 and RAW <2 or FV<0.0001;
- ISSC: 0.001>FV>0.0001 and RAW>2; and
- HSSC: FV>0.005, or 0.005>FV>0.001 and RAW>2.

For the application of IMs to different fields see (Zhou, et al., 2006; Borgonovo & Smith, 2011; Cheok, et al., 1998; Chen, et al., 2007; Mahboob, et al., 2012(b)).

Table 4.1: Selected importance measures and their brief definitions.

Importance measures and their theoretical description	Mathematical definition
Conditional Probability (CP): Gives the $\mathbf{Pr}(\boldsymbol{F_s})$ given the $\mathbf{Pr}(\boldsymbol{F_i})$	$CP_{(i)} = \frac{\Pr(F_s \cap F_i)}{\Pr(F_i)}$
Risk Achievement Worth(RAW): Measures the worth of component $\boldsymbol{F_i}$ in achieving the present level of system reliability	$RAW_{(i)} = \frac{\Pr(F_s \mid F_i)}{\Pr(F_s)}$
Risk Reduction Worth(RRW): Measures the decrease in system unreliability by increasing the reliability of $\boldsymbol{F_i}$	$RRW_{(i)} = \frac{\Pr(F_s)}{\Pr(F_s \mid \overline{F}_i)}$
Diagnostic Importance Factor(DIF): Gives the $\mathbf{Pr}(\boldsymbol{F_i})$ given the $\mathbf{Pr}(\boldsymbol{F_s})$	$DIF_{(i)} = \frac{\Pr(F_s \cap F_i)}{\Pr(F_s)}$
Birnbaum's Measure(BM): Gives the sensitivity of system unreliability w.r.t to the changes in the $\mathbf{Pr}(\boldsymbol{F_i})$	$BM_{(i)} = \frac{\partial \Pr(F_s)}{\partial \Pr(F_i)}$
Fussel-Vesely (FV) Measure: The standard FV failure importance is the contribution of the $\mathbf{Pr}(\boldsymbol{F_i})$ to the $\mathbf{Pr}(\boldsymbol{F_s})$. $\boldsymbol{FV_{(i)} = 1 - \frac{1}{RRW_{(i)}}}$	$FV_{(i)} = \frac{\Pr(F_s) - \Pr(F_s \mid \overline{F}_i)}{\Pr(F_s)}$
Criticality Importance Factor (CIF): Gives the probability that the component $\boldsymbol{F_i}$ has caused system failure given $\mathbf{Pr}(\boldsymbol{F_s})$	$CIF_{(i)} = \frac{\Pr(F_i)}{\Pr(F_s)} \cdot BM_{(i)}$
Improvement Potential(IP): Gives the improvement potential if the failed component is replaced by a perfect one	$IP_{(i)} = \Pr(F_i) \cdot BM_{(i)}$

This work considers eight IMs, see Table 4.1, that already exist in the literature (Borgonovo, et al., 2003; Borgonovo & Apostolakis, 2001; Rausand & Hoyland, 2004; Xing, 2004). To present simple definitions of the IMs, we omit the time t, which is implicitly present in all

of the definitions given in Table 4.1. In the definitions, $\Pr(F_S)$ denotes the probability of the failure of a system, which is computed as a function of the probability of the component denoted by $\Pr(F_i)$.

4.7 Life Quality Index (LQI)

The problem of risk acceptance turns into an economic decision problem when the risks are in the so-called ALARP region (see Figure 4.1) and the objective is to further reduce the risks. For example, should we introduce a safety measure if the individual risk is just close to the risk acceptance level? In this situation one requires additional criteria, which may be based on socio-economic considerations. It implies that the considerations of (changing) socio-economic conditions and accommodation of additional information on factual knowledge, which becomes available over time, can affect the decision-making process. For example, the gross domestic product (GDP) per person, and the life expectancy of a human exposed to danger are important socio-economic indicators. Moreover, one safety measure can be a better alternative in terms of value for money and performance than other safety measures. In this situation, socio-economic considerations such as BCA have been utilized for railway risks. The profitability of a safety technology by quantifying the WTP (from the society point of view) is calculated in a BCA. The WTP is the amount that people are willing to pay to save a human life. The BCA and the WTP approaches are usually accepted methods for valuing the prevention of fatalities. For further reading on the BCA and the WTP and their application to different industries readers are referred to (Evans, 2013; TD, 2000; Aoun, et al., 2012; RSSB, 2006; Evans, 2005). Of course, one can disregard the BCA or WTP for the adoption of safety technology if the aim is to prevent and mitigate train collisions and derailments. The usual reason for the disregard is that a higher safety technology is needed than would be calculated by BCA and WTP. (Often, there is criticism around the ALARP principle as it attaches money to a human life in order to adopt a safety measure.) However, some areas of safety improvement such as upgrading or replacements of level crossings (LCs) are good subjects for BCA (Evans, 2013). BCA takes into account the same parameters for the comparison of profitability of different safety technologies. Identification of such parameters for different socio-economic and geographical conditions and assigning

monetary values (to benefits and costs) of the identified parameters always has complications. BCA becomes difficult if the parameters of the decision problem are not completely known. This motivates investigations into an alternative methodology, called LQI. The LQI treats the risk acceptance criterion as an economic decision problem in an uncertain environment. The LQI establishes a relation between the resources utilized in improving the safety of a system and fatalities that can be avoided by the resources. It offers a rational way of finding acceptable decisions on engineering systems involving risks to human life (Nathwani, et al., 1997; Rackwitz, 2002; Lentz, 2007). For the application of the LQI to different engineering fields we refer to (Straub, et al., 2011; Heredia-Zavoni, et al., 2012; Rackwitz, 2008).

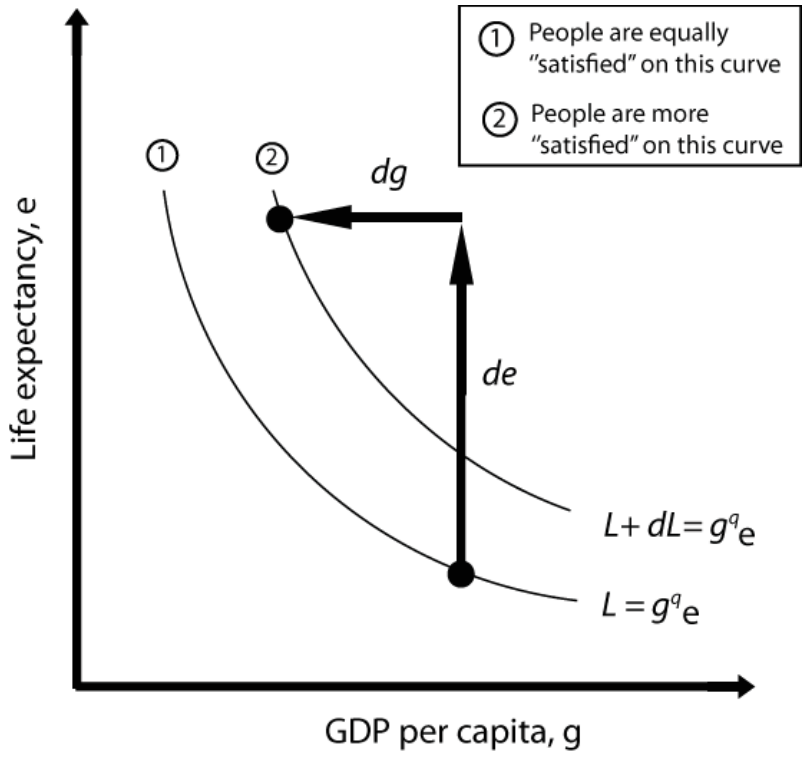


Figure 4.4: Illustration of the Life Quality Index (LQI) principle (Nishijima, 2012).

The LQI is a combined utility function (illustrated in Figure 4.4), which is based on two social indicators; life expectancy at birth, and the real GDP. The strong assumption in the LQI formulation is that people (on average) choose an optimum work-life balance, which is exchangeable. In general, persons may substitute work time for work-free time and vice versa to optimize their total life. For example, in the context of individual risk, one can be willing to accept additional risk of death or injury in the workplace if he or she gets appropriate additional monetary benefits that are appropriate to his or her expected utilities. So, the LQI can be regarded as a utility function, which reflects the net benefits to society.

In this thesis, we do not discuss the mathematical derivations and details of the LQI, but show its application to the railway system, which involves risk. As yet, there has been no any application of the LQI to railway risks.

With few weak assumptions, the formula for LQI (L) can be written as

$$\boldsymbol{L = g^q e}\,. \tag{4.1}$$

In the equation above, e is life expectancy of the safety technology user, the constant parameter q is a measure of the trade-off between the resources available for consumption and the value of the time during the (productive or workable) life. q depends on the part of life allocated for economic activities w and the Cobb-Douglas parameter β for the production function. β accounts for the fact that only a part of the GDP per capita (g) is obtained through work activities and the rest of the GDP is obtained through return investments. q is estimated as follows:

$$\boldsymbol{q = \frac{1}{\beta}\frac{w}{1-w}}\,. \tag{4.2}$$

The general acceptance criteria for a small change in the LQI (dL) due to a safety technology or measure can be assessed by

$$\boldsymbol{dL = \frac{\partial L}{\partial g}\, dg + \frac{\partial L}{\partial e}\, de \geq 0.} \tag{4.3}$$

Fatalities can be minimized and, consequently, life years can be saved if any suitable safety technology is introduced in a railway facility, such as at a railway LC. As a result, a change in life expectancy de at society level will be obtained. The (yearly) cost of a safety technology is expressed as a reduction in GDP dg (money spent on a safety related project such as the installation of an LC barrier). The LQI acceptance criteria implies that the safety technology is implemented as long as

$$\boldsymbol{(-dg) \leq \frac{g}{q}\frac{de}{e}.} \tag{4.4}$$

The (-) with dg in the equation above refers to the cost of installing a safety technology. In general, the decision on safety technology has parallel effects on the risk level and income. For example, safety technology will lead to high average life expectancy e and its cost leads to a decrease in average income g. The societal capacity to commit resources (SCCR), also called societal-willingness-to-pay (SWTP), towards a risk reduction measure is the amount that society is willing to pay to retain its original level of welfare by following a welfare change. A safety technology is accepted if the overall life time utility increases or remains the same. Therefore, the SCCR is the sum received from N persons which, following a welfare change, leaves them at their initial level of welfare. The SCCR for a safety technology is computed as following:

$$\boldsymbol{SCCR = dg \cdot N = N\frac{g}{q}\frac{de}{e}\ €/year.} \tag{4.5}$$

By using the LQI principle, the statistical-value-of-societal life (SVSL) is computed as $1.6 \cdot 10^{06}$ € (Rackwitz, 2004). It should be mentioned that the SCCR type criterion above is applied to risk aversion problems where saving the life of some individual member of so-

ciety is not identifiable in advance. The mathematical relations above for LQI can be calculated from widely available and reliable data for many countries (Rackwitz, 2008), especially, for developed countries where data is easily available. For further details on the mathematical derivations and applications of the LQI approach readers are referred to (Nathwani, et al., 1997; Rackwitz, 2002; Lentz, 2007; Heredia-Zavoni, et al., 2012) and the references therein.

4.8 Summary

ALARP, MEM and MGS risk acceptance criteria are widely applied and accepted in railways. These criteria are used to determine a tolerable level of risk on a railway that can arise due to any technical failure or natural hazard. In order to create a balance between random failures and systematic errors, the SIL approach is used on railways. Based on the tolerable level of the individual or collective risk of fatality, an acceptable level of dangerous failures per hour can be determined using the SIL approach. Brief definitions of different IMs, which are useful in answering a number of questions on system risk, safety and reliability, are given. IMs can be utilized to identify and rank the important components in railways. LQI is an economic based risk acceptance criterion when human life is at risk. It creates a relation between the resources utilized in improving the safety of an engineering system and the potential fatalities that can be avoided by the investment.

CHAPTER 5: APPLICATION OF BAYESIAN NETWORKS TO COMPLEX RAILWAYS: A STUDY ON DERAILMENT ACCIDENTS

5.1 Introduction

This chapter presents an example of a train derailment due to SPAD, which can occur in railways when train passes a red signal. A number of failures and factors can cause SPAD. For example, SPAD can be caused by faulty brakes, high train speed, defective signals and train drivers wrongly reading and responding to cautionary signals. To prevent SPAD, modern railways have automatic signalling and train protection and warning systems. The automatic signalling provides trains the possibility to proceed further and ensure an adequate distance between the trains to avoid accidents. The train protection and warning systems further ensure safe train movement by automatically applying the brakes if the train speed is higher than the permission. The SPAD event can further lead to adverse events such as train derailment. For instance, a train derailment occurs if the turnout/point ahead is not set in the overlap length[3] or the train speed is high, and there is a sharp curve in the overlap length. The train derailment can cause a number of consequences to people, infrastructure, operational processes and environment. The severity of these consequences depends on so-called barriers and neutralizing factors that may exist in between the top event and the consequences. There exist a number of dependencies between the causes of the train derailment. For example, high train speed is a common cause failure; slip and failure towards brake application are disjoint events; failure dependency exists between TPWS and driver errors; driver errors are time dependent and there is functional uncertainty for derailment condi-

[3] Overlap length is provided by positioning the signal some way before (say 200 meters) the entrance to the section it is protecting.

tions. Additionally, accident scenarios (originated from the train derailment leading to consequences) have dependencies due to common barriers and neutralizing factors.

5.2 Fault Tree Analysis for train derailment due to SPAD

A cause consequence analysis, also called safety risk model (SRM) or bow-tie model, which is explained in section 2.7, is shown in Figure 5.1 for train derailment accidents. The causes and the consequences of the *Train derailment* event are modelled using FTA and ETA, respectively. The lower part of the TE in Figure 5.1 is FTA (Mahboob, et al., 2012(d)).

The possible scenarios leading to the TE are shown in the FTA. For example, intermediate event *SPAD* will occur when *Train is approaching a red signal,* and there are (1) combined failures of *TPWS* and *Driver errors*, or (2) *Slip* due to poor adhesion between the rail and wheels. The TE *Train derailment* can occur when the *SPAD* is followed by a (1) a *Turnout/point* with prevented route or (2) a *Curve in track alignment* as well as *High train speed*. It is assumed that the driver has no information on a slippery track conditions. Therefore, the driver is unable to take care of slip related aspects during brake application. The basic events of the scenarios leading to the top event and their frequencies (for illustration only) are summarized in Table 5.1. It is to mention that only *Fixed Unavailability Values* (FUV) and *Failure Frequencies* (FF) are used for basic events in the FTA. The FUV and FF are utilized to represent the probability of failure on demand and simple event probabilities. For example, one driver failure per 1000 brakes application demands, 15 out of 100 trains exceed the speed limit while passing a signal, one failure per hundred thousand demands of TPWS, and every 10^{th} turnout/point is not set in advance.

In general, the probability of TE ($\Pr(TE)$) in the FT is computed as the function of the minimal cut sets by using inclusion and exclusion principle (see Eq. (2.1)) or *de Morgan's law.* The *de Morgan's law* for the ‘*'Union of Events''* is written as[4]

[4] The identity $\Pr(\cap_k E_k) = \prod_k \Pr(E_k)$ only holds for statistically independent events.

$$\mathbf{Pr}(\cup_k \boldsymbol{E_k}) = \mathbf{Pr}(\overline{\cap_k \overline{\boldsymbol{E_k}}}) = \mathbf{1} - \mathbf{Pr}(\cap_k \overline{\boldsymbol{E_k}}) = \mathbf{1} - \prod_k (\mathbf{1} - \mathbf{Pr}(\boldsymbol{E_k})). \tag{5.1}$$

In the equation above, $\Pr(E_k)$ denotes the probability of occurrence of minimal cut set in a FT and k is the number of minimal cut sets. The probability of the TE in Figure 5.1 as the function of the probabilities of the minimal cut-sets is computed as

$$\begin{aligned}\mathbf{Pr}(\boldsymbol{TE}) = \mathbf{Pr}(\, &\boldsymbol{E_1} \cap \boldsymbol{E_3} \cap \boldsymbol{E_4} \cap \boldsymbol{E_7} + \boldsymbol{E_1} \cap \boldsymbol{E_3} \cap \boldsymbol{E_4} \cap \boldsymbol{E_5} \cap \boldsymbol{E_6} + \boldsymbol{E_1} \cap \boldsymbol{E_2} \cap \boldsymbol{E_7} + \\ &+ \boldsymbol{E_1} \cap \boldsymbol{E_2} \cap \boldsymbol{E_5} \cap \boldsymbol{E_6}) = \mathbf{2.84E-04}.\end{aligned} \tag{5.2}$$

In equation above, there are four cut sets, and $E_1 \cap E_3 \cap E_4 \cap E_7$ is one of the four cut sets.

Table 5.1: Basic events for the causes of train derailment and their fixed unavailability (FUV) and failure frequency (FF).

Event	Description	FUV & FF
Train approaching red signal ($\boldsymbol{E_1}$)	Train is running towards a red signal	$5\mathrm{E}-02$
Slip ($\boldsymbol{E_2}$)	Sliding of train (before red signal) over rails due to poor adhesion	$5\mathrm{E}-02$
TPWS fails ($\boldsymbol{E_3}$)	TPWS fail on demand such as while passing a signal	$1E-05$
Driver errors in brake tion ($\boldsymbol{E_4}$)	Driver fails to react to a brake demand in time	$1E-03$
High train speed ($\boldsymbol{E_5}$)	Speed of the train is $>$ 60 Km/hour	$15E-02$
Curve in track alignment ($\boldsymbol{E_6}$)	Railway track is not straight after passing a signal	$1E-01$
Turnout/point not set ($\boldsymbol{E_7}$)	A turnout/point prevents the route after a red signal	$1E-01$

5.2.1 Computation of importance measures using FTA

By making use of Eq. (5.2) one can compute the IMs in Table 4.1. The computation of all IMs for the basic event 1, which is denoted by E_1, is presented here.

Conditional probability (CP): To calculate $\Pr(TE|E_1)$, we put $\Pr(E_1) = 1$ in Eq. (5.2) and get $\Pr(TE|E_1) = 5.75\mathrm{E}-03$.

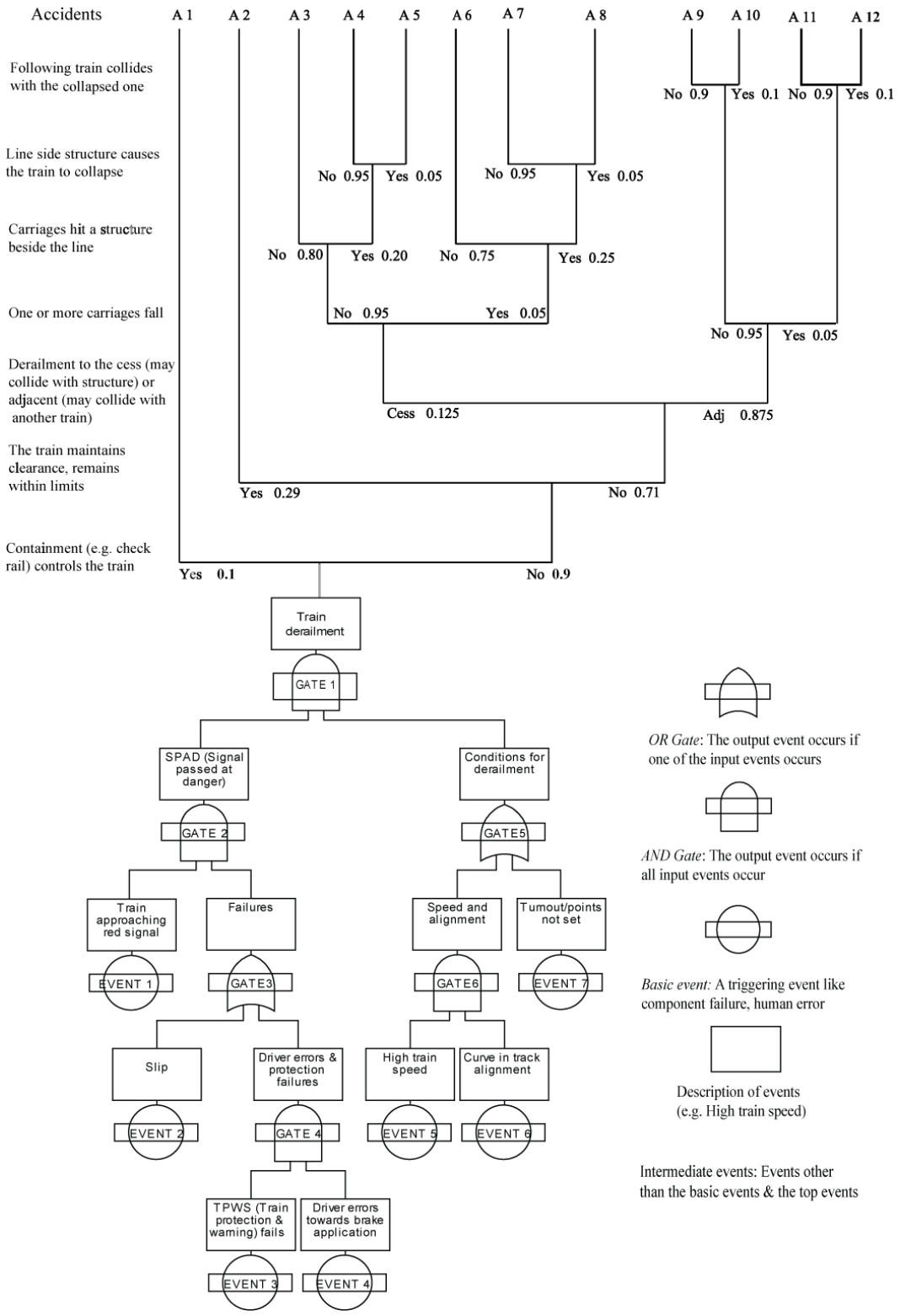


Figure 5.1: A safety risk model for train derailment.

Risk achievement worth (RAW): The calculation of the RAW for individual basic event is straightforward as we have all values for it. We compute $\mathrm{RAW}_{(\mathrm{E}_1)} = 20.$

Risk reduction worth (RRW): We put $\Pr(E_1) = 0$ in Eq. (5.2) for $\Pr(TE|\overline{E_1})$ and pute $\mathrm{RRW}_{(\mathrm{E}_1)}$ as ∞.

Diagnostic importance factor (DIF): The mathematical definition of DIF given in Table 4.1 can be further extended by replacing the term $\Pr(TE \cap E_i)$ with $\Pr(TE|E_i) \cdot \Pr(E_i)$. We get $\mathrm{DIF}_{(E_1)} = 1.$

Fussell-Vesely measure (FV): In standard FV we deal with the minimal cutsets involving the particular event. In this way, the failure importance is measured by taking into account the contribution of the event E_i to the system failure. The FV failure importance measure for basic event E_1 is calculated as 1.

Birnbaum's measure (BM): The partial derivatives of the Eq. (5.2) with respect to $\Pr(E_i)$ gives the $\mathrm{BM}_{(\mathrm{E}_1)} = 5.75E-03.$

Criticality importance factor (CIF): All the values to calculate the CIF for the E_1 are available. We obtain CIF of the basic event as 1.

Improvement potential (IP): The improvement potential with respect to basic event E_1 is calculated by multiplying the $BM_{(E_1)}$ with the$\Pr(E_1)$. We obtain $IP_{(E_1)} = 2.88E-04$. The values of the IMs computed from the FTA are presented in Table 5.2.

Table 5.2: IMs computed from Fault Tree Analysis.

IMs	Event 1	Event 2	Event 3	Event 4	Event 5	Event 6	Event 7
CP	5.75E-03	5.75E-03	2.93E-04	2.93E-04	5.00E-04	6.25E-04	2.54E-03
RAW	20	20	1.02	1.02	1.74	2.17	8.83
RRW	∞	5.07E+04	1.01	1.01	1.15	1.15	7.67
DIF	1	1	1.02E-03	1.02E-03	2.61E-01	2.17E-01	8.83E-01
FV	1	1	1.31E-02	1.31E-02	1.30E-01	1.30E-01	8.70E-01
BM	5.75E-03	5.75E-03	9.50E-06	9.50E-06	2.50E-04	3.75E-04	2.50E-03
CIF	1	1	3.30E-05	3.30E-05	1.30E-01	1.30E-01	8.70E-01
IP	2.88E-04	2.88E-04	9.50E-09	9.50E-09	3.75E-05	3.75E-05	2.50E-04

5.3 Event Tree Analysis (ETA)

Depending on mitigation factors like barriers and neutralizing factors the occurrences of the TE can lead to a number of possible consequences such as damage to the property, deaths, injuries and other economy losses. The upper part of Figure 5.1 is the ETA for the train derailment accident. This ETA is adopted from (Bearfield & Marsh, 2005) where derailment accidents are analysed for UK railways. However, by following IEC 61508 standards (IEC 61508, 2000) the ETA for the train derailment is further extended by introducing SILs, barriers and neutralizing factors for different consequences. The accidents are classified according to their severity levels. (Determining typical severity outcomes in consequence analysis is not always clear in technical systems.) This classification is necessary to differentiate between significant, fatal and insignificant accidents. For example, accidents A1, A2, A3 and A9 do not involve a collision of trains and collapse of individual vehicle and are regarded as insignificant in Table 5.3. The occurrence or not occurrence of the seven events included in the ETA can lead to the twelve consequences (A 1 to A 12). The seven events differentiate the event scenarios within the ETA by representing different branches, which connect the initiating event with its consequences. The seven events and their probabilities are shown in the upper part of Figure 5.1.

Table 5.3: Safety integrity levels (SILs) level for different consequences of train derailment.

Severity class	SIL	Accidents
Insignificant: Minor injuries	0	A1, A2, A3, A9
Marginal: Major injuries	1	A6
Critical: 1 fatality	2	A11
Catastrophic: 10 fatalities	3	A4, A7,
Disastrous: 100 or more fatalities	4	A5, A8, A10, A12

The probability of each consequence is computed by multiplying the probability of the initiating event with the probabilities of the events defining each scenario. For example, the probability of accident A_5 is calculated as $2.84 \cdot 10^{-04} \cdot 0.9 \cdot 0.71 \cdot 0.125 \cdot 0.95 \cdot 0.2 \cdot 0.05 = 2.153 \cdot 10^{-07}$.

5.4 Mapping Fault Tree and Event Tree based risk model to Bayesian Networks

It has been proven that any FT can be translated into an equivalent BN (Khakzad, et al., 2011; Bobbio, et al., 2001). The parts of FT and Bayesian Networks are used for graphical and numerical mappings; a simplified procedure is presented in Figure 5.2.

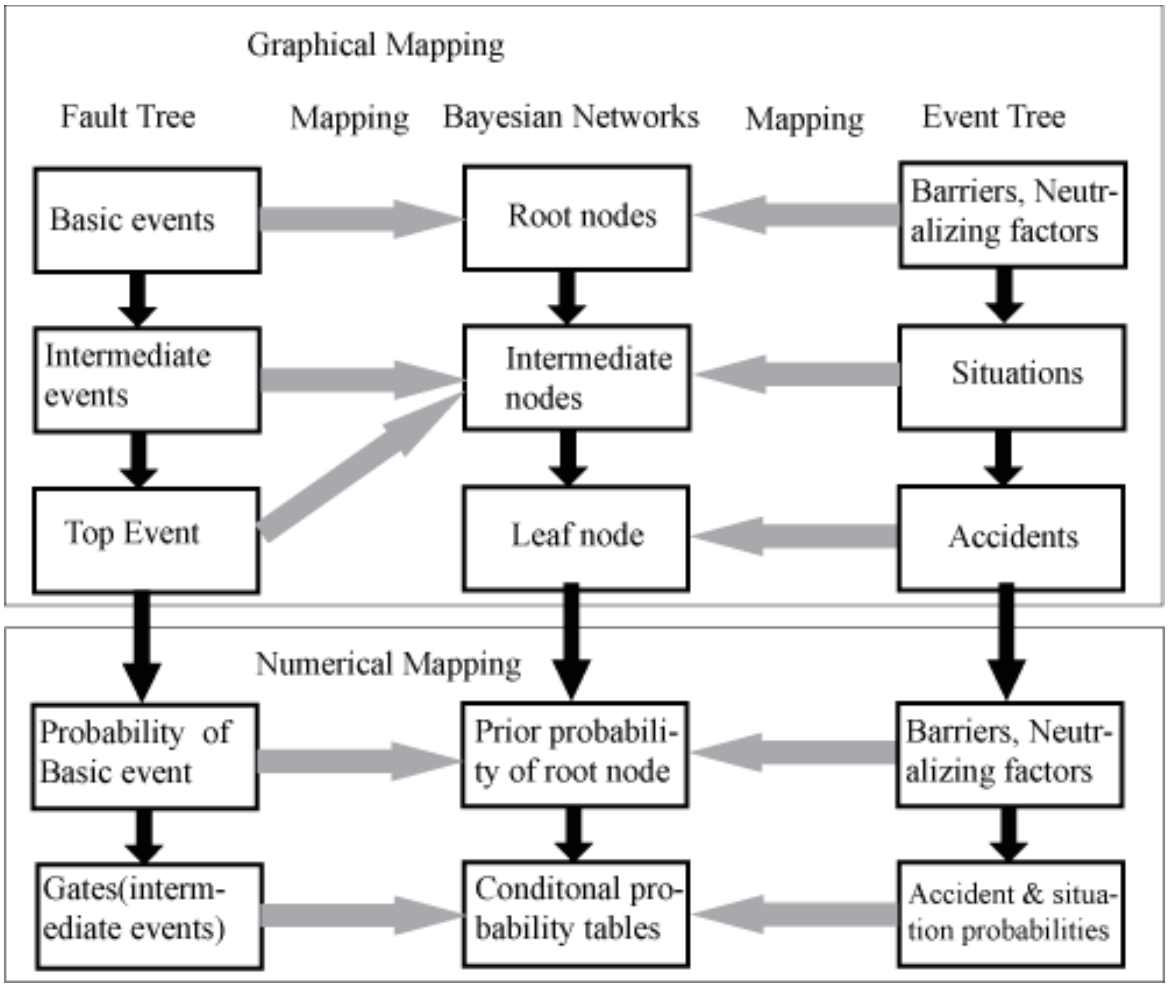


Figure 5.2: Mapping of a Fault Tree and Event Tree based model to Bayesian Network.

For better understanding of the mapping processes, the nodes in the Bayesian Networks are further classified as follows. *Root node of Bayesian Networks:* It is used to represent basic events of the FTA and barriers and neutralizing factors of the ETA. Barriers can be technical or operational measures, which can actively mitigate the hazard evolution to an acci-

dent. Barriers can be characterized by their functionality, occurrence and effectiveness. Neutralizing factors, also called lucky circumstances, mitigate the hazard propagation to an accident, after the barriers have failed. *Intermediate node of Bayesian Networks:* It is used to represent intermediate events in FTA and intermediate scenarios in ETA. *Leaf node of Bayesian Networks:* It is used to represent the output of model; e.g., consequences in ETA.

Keeping in view the properties of the Bayesian Networks and the mapping algorithms above, we represent the complete model from Figure 5.1 into Bayesian Networks, see Figure 5.3. (For simplicity we use shorter names of random variables in Bayesian Networks, say 'Fall' for *One or more carriages fall.)* For instance, the AND logic between the random variables *High train speed (HTS)* and *Curve in track alignment (CTA)* is shown in Table 5.4 for *Speed & alignment (SA)*. The probability of the *SA=Yes* is calculated as

$$\begin{aligned}\mathbf{Pr}(\boldsymbol{SA = Yes}) &= \sum_{\boldsymbol{CTA,HTS}} \mathbf{Pr}(\boldsymbol{SA = Yes} \mid \boldsymbol{CTA} \cap \boldsymbol{HTS}) \cdot \mathbf{Pr}(\boldsymbol{CTA} \cap \boldsymbol{HTS}) \\ &= \mathbf{1.5E-02}.\end{aligned} \tag{5.3}$$

In equation above the basic events *CTA* and *HTS* are statistically independent; meaning that $\Pr(CTA \cap HTS) = \Pr(CTA) \cdot \Pr(HTS)$.

Table 5.4: Numerical mapping of AND gate for speed & alignment (SA) in FT to equivalent probability table in Bayesian Networks.

CTA	**Yes**		**No**	
HTS	Yes	No	Yes	No
Yes	1	0	0	0
No	0	1	1	1

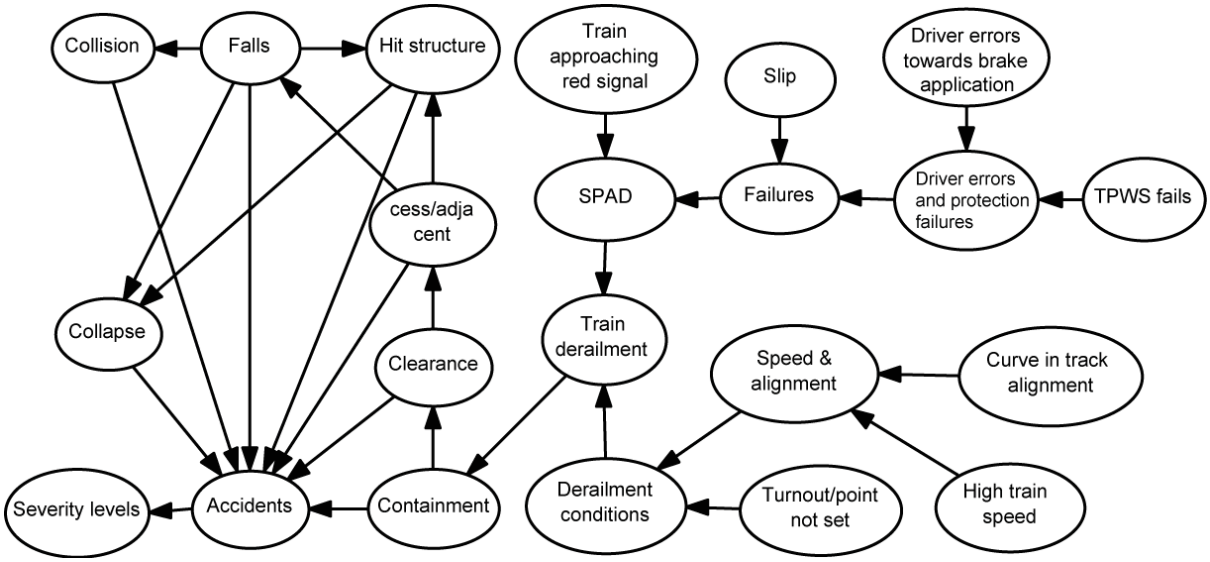


Figure 5.3: Bayesian Networks model equivalent to the FT & ET based model.

5.4.1 Computation of importance measures using Bayesian Networks

The computation of the IMs using Bayesian Networks is shown in (Si, et al., 2011; Mahboob, et al., 2012(d)). However, the computation of IMs for complex engineering systems is not discussed so far. To answer questions related to the marginal and joint probabilities of the random variables in the Bayesian Networks we make use of the standard Bayesian inference using variable elimination algorithm. The variable elimination algorithm involves three steps: (1) pulls out terms form the joint probability distributions of Bayesian Networks by maximizing independence, i.e. using d-separation properties (2) combine together parts of Bayesian Networks to obtain smaller Bayesian Networks with larger terms, i.e. joint probability mass functions and (3) enumerate over these smaller parts of Bayesian Networks. These operations continue until we achieve a desired distribution. In other words, it is a way to determine the distribution of a subset of variables in Bayesian Networks by continuously eliminating the nodes from the Bayesian Networks that are independent of the subset of interest. For further details on the variable eliminations algorithms, readers are referred to (Koller & Friedman, 2009; Jensen & Nielsen, 2007).

The nodes in the Bayesian Networks in Figure 5.3 are assigned the same probabilities as the basic events in the FT. To this end, the Bayesian Networks in Figure 5.3 result in the same probability of the TE and the values of the IMs as in Table 5.2.

5.5 Risk quantification

Next step is to compute the numeric values of the *Individual Risk of Fatality (IRF):* expressed in terms of annual fatality rate for a person, which is exposed to the given (dangerous) situation at a given point in time. It can be calculated as (Braband & Lennartz, 2000):

$$\boldsymbol{IRF} = \sum_{j} \boldsymbol{N}\left[\boldsymbol{HR_j}(\boldsymbol{D_j} + \boldsymbol{E_j})\sum_{\boldsymbol{k}}(\boldsymbol{C_j^k F^k})\right] \tag{5.4}$$

- N= Number of times an individual is exposed to system hazards
- j= Number of hazards
- HR_j= Rate for j^{th} hazard (top event in FTA)
- D_j=Duration time of hazard j
- E_j= Exposure time for an individual towards hazard j
- k = Number of accidents

$\sum_k(C_j^k\ F^k)$= Risk reduction parameters ($C_j^k$is risk reduction factor for k^{th} accident due to j^{th} hazard and F^k is the probability of fatality in k^{th} accident). The risk reduction factor is computed from the consequence models, e.g., ETA.

Fatalities are the main concern in railway risks, therefore; only risk reduction factor C_j^k for accidents corresponding to severity levels 2, 3 and 4 ($0.0278 + 0.0170 + 0.063 = 0.1078$) in Table 5.5 are considered for the IRF. The SIL 0 and SIL 1 categories are not considered in the computation as they do not result, apparently, in human fatalities.

Table 5.5: Risk reduction factors computed from the models.

Severity class	SIL	C_j^k
Insignificant: Minor injuries	0	0.889
Marginal: Major injuries	1	0.0033
Critical: 1 fatality	2	0.0278
Catastrophic: 10 fatalities	3	0.0170
Disastrous: 100 or more fatalities	4	0.063

The other numerical values for the IRF are as follows: $HR = 2.84 \cdot 10^{-04}$ (from FTA), $N = 600$ times per year (on average, an individual uses train two times a day and 300 days a year), $j = 1$ (only one hazard or TE), D_j= 5 hours (average repair or negating time for (hazard situation due to) failure), E_j= 0.05 hour (time for observing and crossing a red signal and overlap length), $C_j^k = 0.1078$ and $F^k = 0.01$. The numeric value of the IRF is $9.28E-04$ Per year . To this end, the numeric value of the IRF is the same from the risk models in Figure 5.1 and Figure 5.3 as they are equivalent. However, these models are based on a number of simplifications, which are identified in the next section.

5.6 Advanced aspects of example application

A number of simplifications in the model in Figure 5.1 are identified. It is argued that this model do not consider a number of so-called advanced aspects, which are usual in railway engineering systems. Failing to consider such advanced aspects will lead to over or under estimation of risks and reliability in such systems.

5.6.1 Advanced aspect 1: Common cause failures

The FT in Figure 5.1 assumes that the basic events are (statistically) independent. This does not hold for the basic events *Slip* and *High train speed.* In order for the slip to occur, a high train speed is required. Therefore, high train speed is a shared cause, also called common cause of failure. When such common causes are ignored, the risks are either (1) overesti-mated if the FT is dominated by series (OR gate) components or (2) underestimated if the FT has many components in parallel (AND gate).

5.6.2 Advanced aspect 2: Disjoint events

The basic events *Slip* and intermediate event *Driver errors and protection failures* cannot occur jointly because slip requires that brakes are applied. These events are mutually exclusive (disjoint) and, therefore, are not statistically independent.

5.6.3 Advanced aspect 3: Multistate system and components

The events of a standard FT correspond to random variables with binary states (fail/success). The FT cannot directly model multistate components or mutually exclusive system states. However, such multistate modelling is often required for representing different conditions of a component or system. For instance, for the train derailment due to SPAD, two different system states, or so-called situations must be distinguished.

Situation 1: SPAD occurs due to slip effect caused by poor adhesion. This implies that brakes are applied when passing the red signal. In this situation, derailment will only occur if the distance between the signal and the turnout point (in the overlap length) is sufficiently small. Otherwise, the train will come to a stop before the turnout point. Derailment due to curvature in the track is negligible since the train speed is already limited by brake application.

Situation 2: SPAD occurs because brakes are not applied, corresponding to occurrence of the intermediate event *Driver errors and protection failures*. In this situation, top event occurs independently of the overlap length due to (1) a turnout in the following section with prevented route and (2) a curve in the following section. It implies that one additionally requires two basic events (see Table 5.6) to model multistate system.

Table 5.6: Basic events for modelling multistate event for train derailment model.

Event	Description	FUV & FF
Poor adhesion	Adhesive forces between train wheels and rails are not enough	0.03
Shorter overlap length	Distance between (last) signal and turnout ahead is $\leq$ 200 m	0.005

5.6.4 Advanced aspect 4: Failure dependency

Failure of one component can lead to an increased or decreased tendency for other components in the system to fail. For example, it is reasonable to consider that the probability of intermediate event *Driver errors & protection failures* will be higher if TPWS fails earlier than driver errors. In other words, probability of driver errors will be higher given that there are TPWS failures.

5.6.5 Advanced aspect 5: Time dependencies

There is time dependent event in the FT. The probability of driver errors increases over time, especially when the driver has to perform longer than regular duty hours. In other words, the probability of the event E_4 will change in time, which will change the probability of the TE over time.

5.6.6 Advanced aspect 6: Functional uncertainty and factual knowledge

There is uncertainty not only about the occurrence of an event, but also on the functional/failure logic (like OR, AND) between the (basic) events. For instance, the failure uncertainty arises when there is a track section, which involves both curve in track alignment and turnout/point not set. There will be an increased tendency for derailment if the train enters into this section, after the occurrence of SPAD. Moreover, the maintenance, repair and replacement actions taken in the past tell that there is no overlap length that has both *Curve in track alignment* and *Turnout/point*. Therefore, the failure logic OR for *Conditions for derailment* must be replaced with XOR (see Table 5.7),

Table 5.7: XOR logic for Conditions for derailment.

Speed and alignment	Yes		No	
Turnout/point not set	Yes	No	Yes	No
Yes	0	1	1	0
NO	1	0	0	1

5.6.7 Advanced aspect 7: Uncertainty in expert knowledge

Where there is not enough historical data to quantify the risks, experts in the field are used to estimate the probability of occurrence of particular events. Sometime, experts do not agree on the probability of occurrence of an event. For example, two experts have different believes on the probability of *Curve in track alignment* that will lead to the TE.

5.6.8 Advanced aspect 8: Simplifications and dependencies in Event Tree Analysis

The ETA in Figure 5.1 simplifies event scenarios leading to the consequences, thus fails to include a number of barriers and neutralizing factors. A detailed presentation of barriers and neutralizing factors in the field of railways is given in (Puettner & Geisler, 2008). For the purpose of the exemplification of the use of Bayesian Networks in the calculation of risks in the railways, only the following barriers and neutralizing factors are considered here.

Barrier 1- Human intervention to avoid an accident: For instance, driver (staff, passengers or third person) observes the situation properly and acts accordingly.

Barrier 2- There is an independent (technical protection) device in the system that has to intervene in case of an accident. For example, slip sidings are provided if the gradient falling away from the signal or station is steeper.

Neutralizing factor 1- Operational environment: It could be unusually low or no trains on the railway network and passengers in the trains. This could also specify characteristics of infrastructure in the environment such as bridge and tunnels. For example, accident close to bridge or in a tunnel can lead to higher consequences.

Neutralizing factor 2- Human exposure and attention: For example, no exposure of person in hazardous area or human is attentive in case of a hazardous situation.

Depending on the system characteristics, there could be some neutralizing factors and barriers in the ET that are equally valid for the FT. In other words, there are neutralizing factors and barriers that can prevent both hazard occurrence and its propagation. However, dependencies among neutralizing factors and barriers are not considered here. Moreover, the prior probabilities of every single neutralizing factor and barrier are assumed to be 0.1.

Some of the advanced aspects discussed above can be implemented using advanced FTA techniques (Xing & Amari, 2008). However, in most cases the structure of the FT increases exponentially and also becomes nonintuitive. For example, by including three advanced aspects: common causes, disjoint events and multistate system, into the model, the structure of the FT is as in Figure 5.4. In other words, the structure of a FT can become different if a new common cause is introduced. The quantitative analysis of the FTA becomes computationally demanding and requires the aid of computerized methods for its evaluation. For example, due to repetition of gates in the FT in Figure 5.4 the common causes have increased to six. In this way, we require 2^6 common cause event spaces (CCE) to compute the probability of the TE. The probability of the TE will then be calculated using the total probability theorem:

$$\mathbf{Pr}(\boldsymbol{TE}) = \sum_{\boldsymbol{i=1}}^{\boldsymbol{2^6}} \mathbf{Pr}(\boldsymbol{TE}|\boldsymbol{CCE_i}) \cdot \mathbf{Pr}(\boldsymbol{CCE_i}). \tag{5.5}$$

Moreover, a previous study show that one cannot model advanced aspects like functional uncertainty and expert knowledge using FTA (Khakzad, et al., 2011). Although, it is possible to include neutralizing factors and barriers in the ETA; however, there exist structure explosion problem with an increase in mitigation factors and dependencies among them. These limitations on the modelling and analysis of the advanced aspects in railways risk and reliability can be solved using the Bayesian Networks approach.

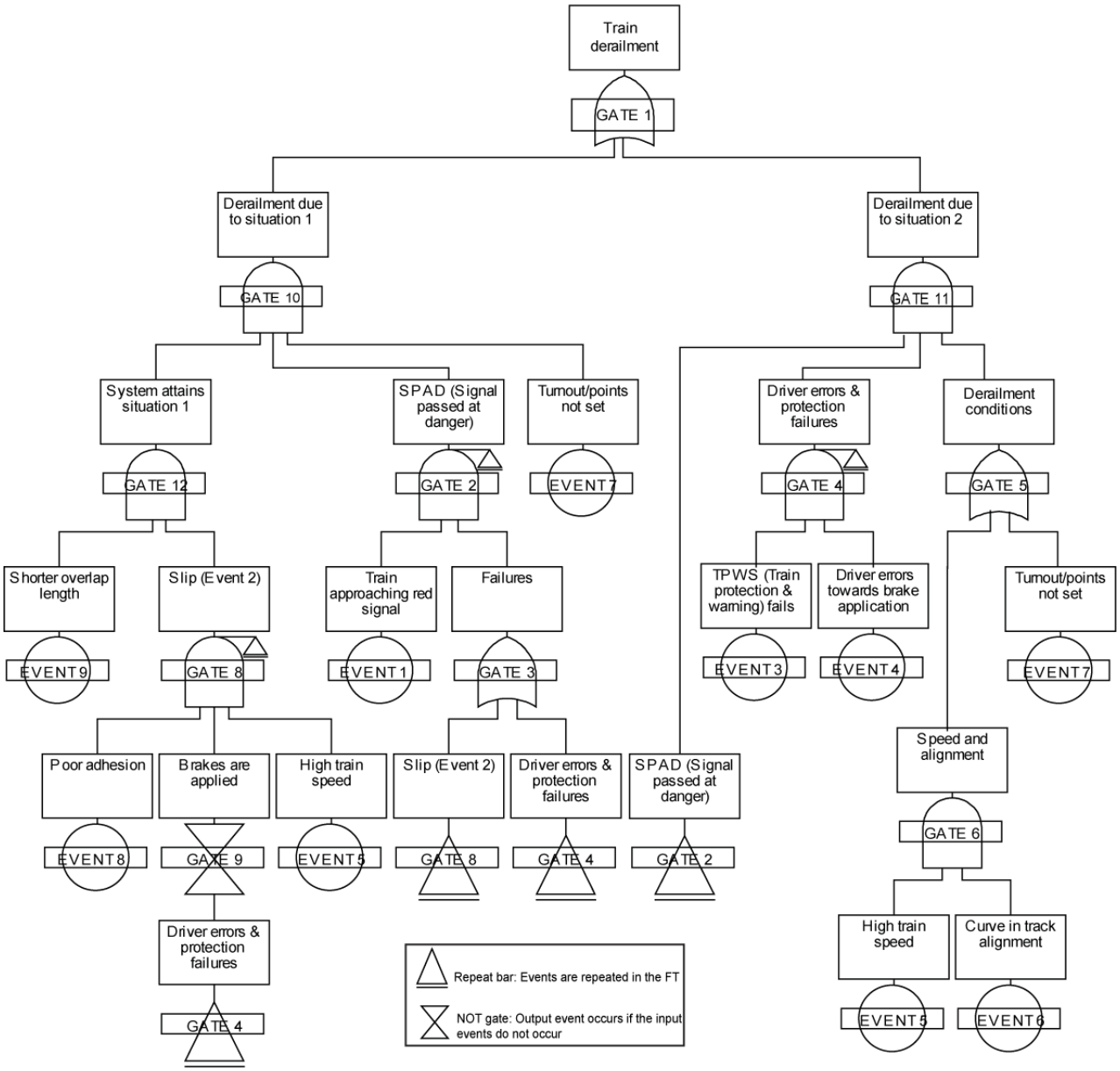


Figure 5.4: Fault Tree Analysis of Train Derailment after considering three advanced aspects.

5.7 Implementation of the advanced aspects of the train derailment model using Bayesian Networks.

The methodology to map the FT & ET based safety risk model to Bayesian Networks is explained above. This section shows how the advanced aspects explained in above are implemented using Bayesian Networks. In the Bayesian Networks, the common causes can be

directly introduced by adding corresponding links, without repeating the nodes. The common cause *High train speed* is accounted for by introducing the link from *High train speed* to *Slip* and *Speed and alignment.* Modelling of disjoint events is managed by adding a link between the corresponding random variables and then inserting the values in the conditional probability table of the child node accordingly. For example, the event *TPWS failure and driver errors* and the event *Slip* are mutually exclusive as discussed above. A link is added from the node *TPWS failure and driver errors,* and the probability of slip given *TPWS failure and driver errors* is set to zero (compare column 2 and column 3 of Table 5.8).

Table 5.8: Conditional probability table for node slip.

High train speed	**Yes**				**No**			
Poor adhesion	**Yes**		**No**		**Yes**		**No**	
TPWS & driver errors	Yes	No	Yes	No	Yes	No	Yes	No
Slip	0	1	0	0	0	0	0	0
No slip	1	0	1	1	1	1	1	1

The multistate system can be represented directly by introducing corresponding random variable *Situations* in the Bayesian Networks. The conditional probability table for two situations is shown in Table 5.9. The missing values in the columns mean that these events cannot occur together. Failure dependency among system components (random variables in Bayesian Networks) can also be managed by using conditional probability table attached to child nodes. For example, column 3 of Table 5.10 shows the increased tendency of occurrence of *TPWS fails and driver errors* when the event *TPWS Fails* occurs earlier than the driver errors. Previously, in the FT model shown in Figure 5.1, it was treated as an AND gate.

Table 5.9: Conditional probability table for node situations.

Overlap length	**Yes**				**No**			
TPWS fails & driver errors	**Yes**		**No**		**Yes**		**No**	
Slip	Yes	No	Yes	No	Yes	No	Yes	No
Situation 1	-	0	1	0	-	0	0	0
Situation 2	-	1	0	0	-	1	0	0

Table 5.10: Conditional probability table for TPWS fails and driver errors.

TPWS Fails	Yes		No	
Driver errors towards brake application	Yes	No	Yes	No
Yes	1	0.05	0	0
No	0	0.95	1	1

A temporal node is introduced to model time dependence of driver errors. The temporal node Driver error towards brake application (DE) is attached with a conditional probability table, which evolves over time and is utilized to model transition probability. The transition period is considered to be 10 minutes (equivalent to 10^{th} order Markov chain in the Bayesian Networks in Figure 5.5). Here, $p(\,DE_t \mid DE_{t-10}\,) = 1$ and $p(\,DE_t \mid \overline{DE_{t-10}}\,) = 0.005$. To model functional uncertainty, the conditional probability value $p(Train\ derailment \mid SPAD, Speed\ \&\ alignment,\ Turnout/point\ not\ set) = 0.1$ is assigned to a table attached to the node *Train derailment*. Modelling of factual knowledge using Bayesian Networks is straightforward, by attaching a conditional probability table to the node Derailment conditions and using XOR logic as shown in Table 5.7. A node called Expert knowledge is introduced in the Bayesian Networks and the probabilities of Curve in track alignment conditional on the states of this node are defined. The probabilities of Curve in track alignment given Expert 1 and 2 are 0.1 and 0.2, respectively. Moreover, reliabilities of the two experts on their judgment can be included. For example, one consider that expert 1 is higher reliable than the expert 2 and, therefore, assigns their probabilities as 0.55 and 0.45, respectively. The barriers and the neutralizing factors can be included by introducing only two nodes called Barriers and Neutralizing factors in the Bayesian Networks, and making consequences dependent on them through the conditional probability table attached to the node Accidents. The resultant Bayesian Networks after the implementation of the advanced aspects is shown in Figure 5.5.

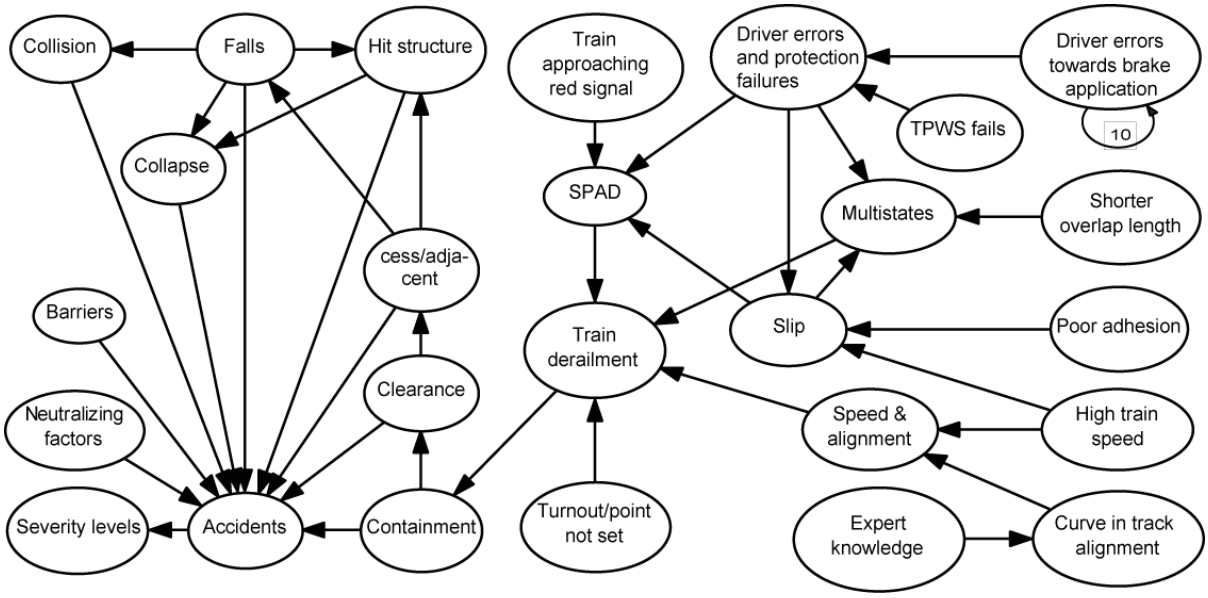


Figure 5.5: Bayesian Networks based safety risk model including advanced aspects of the FT & ET based safety risk model.

The computation of the IM values for Bayesian Networks in Figure 5.5 is also straightforward by using variable elimination algorithms for probabilistic inference. However, this time we obtain different values of the IMs, see Table 5.11.

Table 5.11: Values of importance measure from Bayesian Networks after advanced aspects.

IMs	Event 1	Event 2	Event 3	Event 4	Event 5	Event 6	Event 7
CP	8.05E-06	2.17E-05	3.05E-04	6.08E-06	1.24E-06	6.10E-07	3.53E-06
RAW	20	5.40E+01	7.57E+02	1.51E+01	3.08	1.52	8.76
RRW	∞	1.32	4.11	1.01	1.58	1.10	7.26
DIF	1	2.70	7.57E-01	1.51E-02	4.62E-01	1.52E-01	8.76E-01
FV	1	2.40E-01	7.57E-01	1.41E-02	3.67E-01	8.74E-02	8.62E-01
BM	8.05E-06	2.14E-05	3.05E-04	5.68E-06	9.85E-07	2.43E-07	3.47E-06
CIF	1	2.66	7.57E-01	1.41E-02	3.67E-01	6.03E-02	8.62E-01
IP	4.02E-07	1.07E-06	3.05E-07	5.68E-09	1.48E-07	2.43E-08	3.47E-07

5.8 Results and discussions

We obtained the same IM and IRF from the risk models in Figure 5.1 and Figure 5.3; because, they are equivalent in logic and use the same probability values for their events. However, the probability of the TE is reduced to $4.02 \cdot 10^{-07}$ in the Bayesian Networks model in Figure 5.5. The numerical value of the IRF is recomputed using the Bayesian Network model with advanced aspects, and the new value is $3.787E-07$ per year. The IRF has been reduced due to the high values of the risk reduction factors for consequences. It implies that the risk models without advanced aspects overestimated the system risks. The reliability related IM values of many events in the Bayesian Networks in Figure 5.5 have been changed. For instance, RAW identifies the increase in the system risks if a particular event in the system has occurred. The RAW of the basic events 2, 3, 4 and 5 have been increased in Table 5.11 compared to their values in Table 5.2. RRW identifies the decrease in system risk if the component is assumed to be perfectly working. The RRW of the basic event 2 has been considerably increased in Table 5.11. FV gives the fractional contribution of an event's occurrence towards system failure. An increase in the occurrence probability of the event will lead to an increase in the FV value. The FV values of the basic events 2, 6 and 7 have been decreased whereas the FV values of the basic events 3, 4 and 5 have been increased in Table 5.11.

The FT cannot offer diagnostic analysis (backwards updating), which gives important information about the most probable cause of a certain TE, say $\Pr(E_1 \mid E_6)$. In the FT, each TE has to be analysed at a time, using different FTs for different TEs. Apart from the Bayesian Networks offering computation of the IMs for the complex system model, the additional benefit in using Bayesian Networks was that they modelled joint distributions of random variables in a compact way, leading to a concise visualization of the risk and reliability problem. Bayesian Networks can update the probabilities, so-called beliefs of each random variable in the Bayesian Network, via bi-directional (forwards & backwards) propagation of evidence through the whole network. The two ways of updating enable Bayesian Networks to handle a large number of TEs. In other words, each node in the Bayesian Network can be treated as an independent TE and thus can be evaluated in the Bayesian Network framework. In importance analysis, this backwards updating can be important as it will signify the characteristics of a risk and reliability problem. By exploiting the use of updating character-

istics of the Bayesian Network, the idea of importance analysis for complex systems can find new developments and definitions since they can account not only for the components that are down but also for those that are up at the same time. Moreover, incorporating more TEs and the eventual interrelated aspects of these TEs, an integrated picture of the risks characterizing the system risks and reliability can be obtained. Some of the advanced aspects mentioned above have been discussed in (Khakzad, et al., 2011) for process facilities, using Bayesian Networks.

5.9 Summary

A number of advanced aspects and their effects on the quantitative risk and reliability analysis of a complex railway problem were studied. The implementation of the advanced aspects using FT, ET, and Bayesian Networks was investigated. The FT and ET based model has limitations in handling a number of dependencies and uncertainties in complex railways. In most cases, the structure of the FT increases exponentially and becomes non-intuitive and computationally demanding. The FT and ET based models are useful for the risk and reliability problems that have few TEs and few dependencies and uncertainties among the events leading to the TEs. Moreover, logical visualization of the system architecture is needed, qualitative analysis is part of the risk and reliability analysis and no integration of new information and (backward) updating are required.

Bayesian Networks offered a suitable probabilistic graphical structure for incorporating a number of dependencies and uncertainties related to the train derailment problem. The implementation of the advanced aspects was possible using a Bayesian Network and the computation of the IMs for the complex system was straightforward. A Bayesian Networks with advanced aspects resulted in different values of the fatality risks and the IMs. Bayesian Networks were able to handle a large number of TEs, intermediate events, uncertainties and dependencies in complex railways in concise and flexible way.

CHAPTER 6: BAYESIAN NETWORKS FOR RISK-INFORMED SAFETY REQUIREMENTS FOR PLATFORM SCREEN DOORS IN RAILWAYS

6.1 Introduction

This chapter presents how to quantify the risk-based safety integrity requirements for a PSD (Platform Screen Door) system in a typical megacity. Urban rail transit systems (URTS) in mega cities are subject to different hazards, which can lead to life safety risks. It motivates transport researchers to prepare for the growing risks, which mega cities pose to its URTS. For instance, the higher the number of users of a URTS, the greater the life safety risks will be, provided that an accident occurs due to any reason. PSD is increasingly utilised to minimise the life safety risks at the interfaces of over occupied trains and platforms in mega cities. Falling of passengers, which are waiting for a train on crowded platforms, can be prevented, and potential fatalities can be avoided if the PSDs are installed along the edge of railway platforms, see Figure 6.1. These doors on platform remain closed when there is no train on the track in front of the platform. The planners and engineers try to identify the safety requirements a PSD system has to fulfil under specific operational, environmental and socio-economic conditions. In the railways, these safety requirements are considered with SILs. The SIL requirements must be agreed by all stakeholders such as operator, manufacturer, regulator and independent assessor. The role of independent assessor is crucial in the certification of SIL requirements (Trinckuaf, 2013(a); Trinckauf, 2013(b)).

This study proposes a generic framework to assess the life safety risks in URTS and how it can be applied to determine the SIL requirements for a safety technology. A case study is presented on the PSD system, which aims to minimise the life safety risks in URTS. The steps in the risk-informed safety requirement process, shown in Figure 6.2, will be ex-

plained in the coming sections for the PSD system. A number of hazardous situations related to a PSD system are identified. A preliminary cause and consequence analysis is carried out to scrutinise the most important hazardous situations. The consequences of these most relevant unwanted events are modelled for specific operation and environment conditions. The identified consequences are quantified and then compared to risk acceptance criteria for assessment. The risk-informed SIL requirements are determined for the PSD system.

Figure 6.1: A platform screen door system installed at the Sao Paulo, Brazil

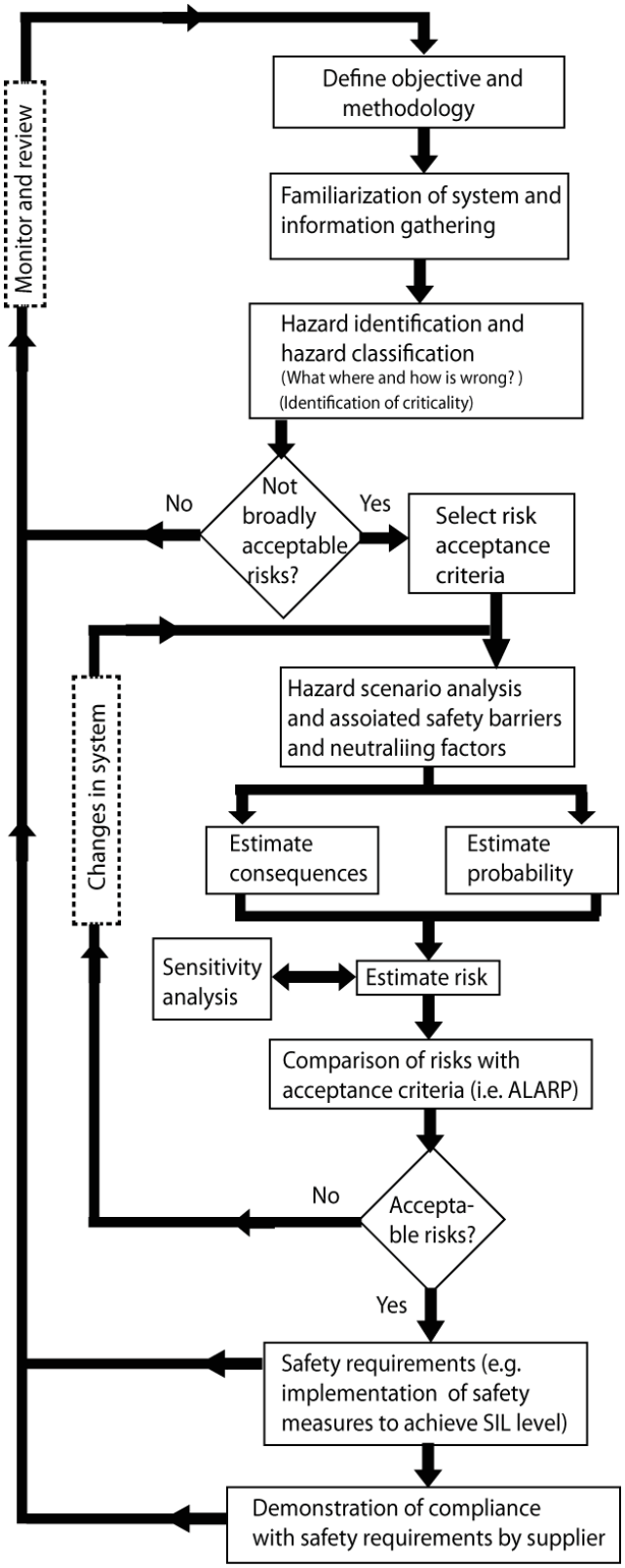


Figure 6.2: Components of the risk-informed safety requirement process for PSD systems (Mahboob, et al., 2013).

6.2 Components of the risk-informed safety requirement process for Platform Screen Door system in a mega city

The components of the risk management processes, which are illustrated in Figure 6.2, are briefly explained in the following sub-sections.

6.2.1 Define objective and methodology

Main objective of the study was to identify and quantify the life safety risks, or so-called fatality rate, associated to the PSD failures. It was aimed to investigate the acceptability of such fatality rate for a particular operating condition. The key elements of the basic methodologies for determining the SIL for PSD are adopted from the standard probabilistic risk assessment (PRA) processes for the nuclear industry. The PRA are well explained in (Modarres, 2008; Aven, 2012) and references therein.

6.2.2 Familiarization of system and information gathering

It was important to know about the functioning of technical system and its operational environment. Thus, a broad knowledge of typical PSD functioning, physical layout of the platform, critical barriers, passenger demands, operational conditions, emergency safety systems, and human interactions was gathered. Functional descriptions and planning configurations of PSD installations provided by a manufacturer/supplier were studied. This step required a comprehensive consultation among supplier, independent assessor and operator of the URTS.

6.2.3 Hazard identification and hazard classification

A total seventeen possible hazardous situations, which will have potential to affect the human and system safety, were postulated. A preliminary hazard analysis (PHA) was carried out with the consultation and support of system manufacturer and operator, see Appendix 1. It was concluded that not all hazardous situations will lead to severe consequences such fatalities. The intention of the PHA was to identify the key hazardous events from the hazard list. The three most relevant hazardous situations (H_1, H_2, H_3 corresponding to hazard ID 11,

12 & 14 in Appendix 1) and their possible consequences (such as fatalities) were identified. H_1 occurs when the PSD opens immediately (due to any hardware or software failure) before a train has approached the platform. H_2 arises when a train starts departing whilst the PSD remains open. H_3 occurs when the recycling (in opening and closing) of train doors occurs. In the third situation, a person can be trapped in between the train and PSD. In the three situations above, a fatality can be anticipated if the train starts moving. During the preliminary analysis, it was concluded that all other hazardous situations are not relevant for the life safety risks associated to the PSD; therefore, only the three main hazards above were discussed in detail.

6.2.4 Hazard scenario analysis

We need to determine the risk reduction parameters first. In order to calculate the risk reduction parameters, one needs to postulate the event scenarios. These event scenarios originate from the hazardous situations and will lead to some consequences including fatalities. All possible scenarios that can initiate from the hazardous situation and lead to fatalities are identified. The logic between the event scenarios is introduced for the three most significant hazardous situations. To achieve this, we use Bayesian Networks approach. Depending on shaping factors (situations, barriers and neutralizing factors) the TE (hazardous situation) can cause a number of possible consequences. These may include damage to the property, deaths, injuries and other economy losses. However, main concern here is the fatality risks. We developed Bayesian Networks based consequence model for the three most relevant hazardous situations (represented with H_1, H_2, H_3 in Appendix 1), shown in Figure 6.3. In the event scenario developments, we considered very low or zero probability values for barriers or neutralizing factors. In other words, worst case assumptions were taken into considerations. For example, we put the probability of *''Emergency measure exists''* equal to zero. The events in the consequence model and their probabilities are explained in next section.

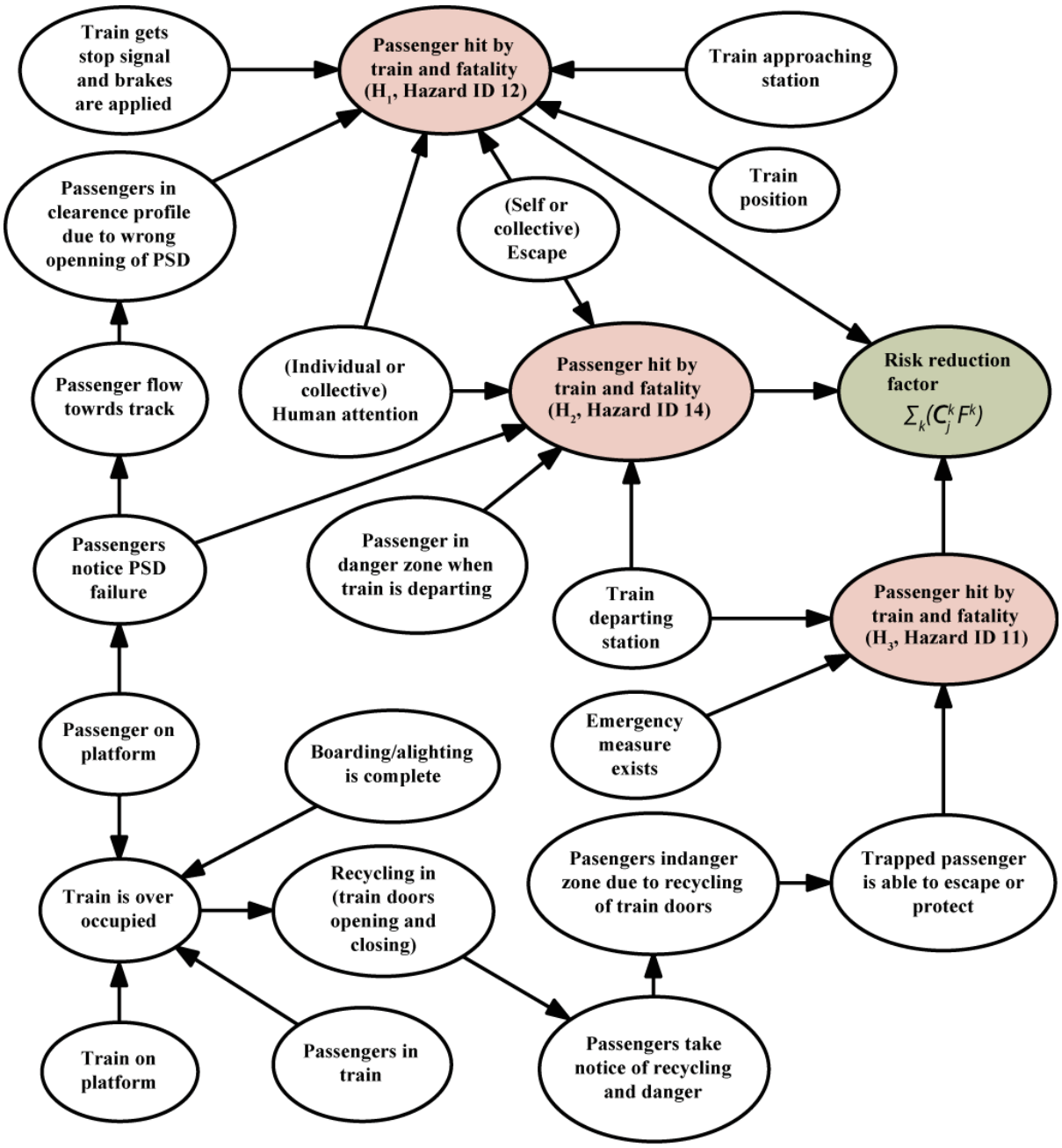


Figure 6.3: Bayesian Networks based consequence analysis for risk reduction factor.

6.2.5 Probability of occurrence and failure data

It is to mention that determining the failure probabilities for different events in the consequence model was a difficult task. There exists no reliability and failure related data for a

PSD; because, it is a relatively new safety technology. (Unavailability of risk and safety related data is a usual problem in many engineering risk and safety assessment problems including railways.) Therefore, failure frequency and unavailability of the events in the Bayesian Networks were intensively discussed among supplier, assessor and operator before their use. How we determine the probability values of the events is explained in the following. It is to mention that all probability values are based on peak hour (operational) demands of a typical URTS in a mega city.

Passengers on platform: Presence of passengers on a platform is necessary for fatality risks, given that failures in PSD occur. We define probability of passenger on a platform as 1. It is assumed that there will be always around 200 passengers at one platform side during peak hour's operation. With 200 passengers per train per side of the platform, we get $200 \cdot 55 = 11000$ passengers per platform side in a peak hour. (There are 55 trains per hour; it is explained in the following.) In this way, one platform has peak demand capacity of 22000 passengers per hour that was according to the operator's requirement.

Passengers notice PSD failure: There is a possibility that passengers take notice of failure (that corresponds to premature opening) in PSD and avoid moving towards trackside. It is mainly based on user's education, training and experience towards the use of PSD. Here, we consider that every 4^{th} person takes notice of a PSD failure (probability 0.25). In other words, one out of four persons observes that the PSD has opened without arrival of the train and will avoid forward movement.

Passengers flow towards track: It depends on the behaviour/attitude of users. In general, people standing at platform wait for people in train to leave first. However, there may be situation (such as mega events) when people at platform do not wait for people in train, but try to board on the train first. We consider 0.5 probability of passenger flow towards track, provided that PSD is opened.

Passengers in the danger zone: Here the assumption is made that 50% out of 200 passengers will not proceed for the very 1st coming train. They intend to take second or later trains. In this way, 100 passengers are supposed to board on every coming train. Moreover, 80% (out of 100 passengers that are supposed to take first coming train) will flow towards track and will remain in clearance profile – probability 0.8. Only 10% ($= 100 \cdot 0.75 \cdot 0.5 \cdot 0.1 \approx$

3 persons) will fall on track due to push, negligence and so on. In other words, (based on above considerations) the probability of a person falling on the track per door is $3/24 = 0.125$.

Individual or collective human attention: This includes apprehension of danger from passengers, emergency and security people available nearby, camera monitoring and so on. The feeling of danger will raise individual and collective attention. We consider the probability of attention as 0.9. The high probability implies that there will be a large number of people available in surroundings during a peak hour or special events.

Self or collective escape: Saving a person in the danger zone (on track or in clearance profile) depends on (1) right individual or collective action and (2) time available for reaction. The headway (65 sec) is so small, therefore; one can assume that the probability of self or collective escape is 0.5.

Probability of a train arriving, departing and on the platform: By considering 65 sec of headway, we can have $3600 \frac{\text{sec}}{\text{hour}} \cdot \frac{1 \text{ train}}{65 \text{ sec}} = 55 \text{ trains per hour}$. We assume that a train takes 36 seconds (3 sec in door opening + 3 sec in door closing + 30 sec in boarding & alighting) to accomplish the service tasks at a platform. In this way, the probability of a train on the platform will be $\frac{36 \text{ sec}}{\text{train}} \cdot \frac{55 \text{ trains}}{3600 \text{ sec}} = 0.55$.

Here, boarding and alighting of 200 persons per train (in 30 sec) is considered. It means every door will have to board/alight $200/24 \approx 9$ passengers in 30 sec. (There are 06 vehicles per train and each vehicle has 04 doors.) It is to mention that 200 passengers will be moving from both sides i.e. from platform to train and train to platform. In this way, total passenger demand that will be dealt by all trains in one hour becomes $200 \cdot 55 = 11000$ passengers per one side of the platform. For two sided platform, the demand will be 22000 passengers per hour, meeting the specifications requirements from the operator. The probability that there is no train standing at the platform is $1 - 0.55 = 0.45$. We split this 0.45 probability in the following way.

Probability of train arriving at station = 0.1. According to this probability a train will take approximately 7 sec from beginning to end of a platform to arrive at a station. Based on 7 sec arrival (and 7 sec for departure) times we get $(55 \, trains \, per \, hour \cdot \frac{7 \, sec}{3600 \, sec/hour}) \approx$

0.1. The velocity of train at the beginning of platform (v_{i}) will be approximately 20 $\frac{\mathrm{m}}{\mathrm{sec}}$ $\left(=\frac{\mathrm{S}}{\mathrm{t}}=\frac{136}{7}\right)$. Length of the platform is 136 m here. In this way, deceleration of train in platform region will be $-\frac{1.4\ \mathrm{m}}{\mathrm{Sec}^2}$ (using equation $2as = v_f^2 - v_i^2$). High deceleration will be required to achieve the maximum number of trains with reduced headways. The *inter-arrival probability* is $(0.45 - 0.1 - 0.1) = 0.25$.

Train gets stop signal and brakes are applied: An approaching train will get a stop signal if the PSD has opened wrongly. In this case, brakes will be applied, and train movement will be halted. We assume that an approaching train will not be able to apply brakes (due to brake failures, no detection or information on PSD failure and other errors) right in time in 1 out of 10 PSD failures.

Train position: There is still possibility that the train can be stopped safely if brakes are not applied right in time after PSD failure. For example, there can be a driver together with the automatic train operation. (It is possible to introduce a driver in driverless trains. It is for additional safety during mega events.) The driver ensures further safety by visualisation and taking in control some safety related operations. In this case, the driver will observe that the PSD remain open and/or a person falling on the track or moving into the clearance profile (danger zone) and applies the brakes. There can be additional monitoring devices like bio-detectors in track environment that can sense bio-mass and give signalling system command to stop the approaching train. We take the probability of a safe stop of the train (after no application of brakes well in time) as 0.1.

Passenger hit by train: There is the possibility that a passenger inside the danger zone can avoid collision with the moving train. In other words, some neutralizing factors may exist. For example, a passenger that has fallen on track can lay down himself on track below the moving train; hide himself below the extended portion of platform or (depending on infrastructure conditions) can find other emergency escape or neutralizing factor. We take this probability as 0.5.

Probability of fatality given passenger hit by train: It is not always the case that the passenger is killed after hit by a train. There can be other consequences like leg or arm broken or

other serious injuries that are other than death. However, we assume that every person hit by train will be dead (may be after some time).

In the event tree for Hazard H_3 (number 11 in Appendix 1), we utilize very conservative values. In other words, high probability values for events in Bayesian Networks are attached.

Passengers in the train: We take probability of passengers being inside the train as 1 because of the metropolitan environment.

Boarding/alighting complete: The probability that the boarding activities are finished is 0.1. It is due to the fact that the train is standing there for a total of 36 seconds. The door closing time is 3 seconds. So we get the probability that boarding is completed $(3\ sec/36\ sec) \approx 0.1$.

Train is over occupied: Over-occupation of the train is necessary for the fatality risks in H_3. Because, passenger will only be pushed outside the train once the train is fully occupied by passengers. However, it is not usual that every train or every vehicle of the incoming train is over occupied in a way that the passenger will be pushed out of the train once the recycling of train door occurs. Therefore, we consider that every second train is over occupied.

Recycling of train door occurs: It is assumed that one out of 24 (≈ 0.05) train doors per train require recycling during the peak demand time. If we consider recycling time 3sec for each train then the total time ($55 \cdot 3 = 165$ sec) will have effects on head way; meaning that the number of trains per hour must be reduced from 55. However, we consider high values.

Passenger takes notice of recycling and the danger: It is usual that passengers take notice of the recycling of train doors, although it depends on the passengers travelling experience. It is assumed that every second passenger standing in front of the train door will take notice of the recycling process. Therefore, this probability is taken as 0.5.

Passenger in the danger zone (between train door and PSD): Probability of passenger in the danger zone depends on the infrastructure conditions. If the space between the train doors and the PSD is high then the probability of a passenger in the danger zone will also be high. We consider three infrastructure scenarios here. The probability that the space between the train door and the PSD is less than 15 cm is 0.55. The probability of the gap is in between 15 cm and 40 cm is 0.3 and for values higher than 40 cm is 0.15.

Passenger is able to escape or protect himself: It is possible that the person trapped in between the train door and the PSD can protect himself or herself in case of being in the danger zone. The probability of protection depends on infrastructure conditions above. For example, in case of the first scenario above (when there is little ($\leq$ 15 cm) space in between the train doors and the PSD) an adult passenger will be protected automatically. The space ($\leq$ 15 cm) is not sufficient to absorb a complete person. It is due to the fact that the train doors will not be closed (after recycling); because, the passenger is almost in between the train doors. The little space between the train and PSD will force recycling to repeat. Meanwhile, the passengers will be able to protect the trapped person. For a little child, it is possible to get trapped between the doors; therefore, we assume that 1 out of 500 passengers is a child with sufficient dimensions to get trapped (probability 0.002). Children are assumed not to be able to escape this situation.

In the second scenario, the space is between 15 cm and 40 cm. There is very little probability (0.05) of escape; because, passenger can easily be absorbed in this space and the repetitions in the recycling of train doors will be less likely due to no hindrance.

In the third scenario, there is enough space for the passenger to keep him away from the train doors. There is 0.5 probability that the passengers cannot protect themselves in this zone.

Emergency measure exists: We take probability that emergency measure exists as zero, because of worst case assumptions.

Train departs (given hazard): Assumption is made that one out of 10 trains will be able depart given that a hazard has occurred. We consider that in 90% of the cases, the train will not depart due to human attention and help of other passengers (emergency brake), camera monitoring systems and so on.

Collision of passenger with train & fatality: The probability of fatality given collision is taken as 0.5. The low probability (as compare to H_1 and H_2) of fatality given collision in this hazardous situation is based on considerations that this is side collision, not head-on collision.

6.2.6 Quantification of the risks

6.2.6.1. Tolerable risks

The most common principles for the determination of risk tolerability are explained in Chapter 4. According to the demands of the risk acceptance criteria, we chose *Tolerable Individual Risk (TIR)* of fatality for a single metro-user as 1E-07 per year. This seems to be a reasonable assumption on tolerable level of risk as it is a much lower rate than normal life safety risks.

6.2.6.2. Risk exposure

The classical way to quantify risks arising in a railway system is to compute *Individual Risk of Fatality (IRF)* (Mokkapati, 2004). We utilise Eq. (5.4) to compute the *IRF*. The data required to compute the *(IRF)* is given below. An individual uses the PSD system, which has *j* hazards. From each hazard, one or several types of accidents may occur. The usage profile is described by the number of uses $N(\text{per year})$ or, in other words, the number of times an individual is exposed to the system hazards. Additionally, for each hazard a hazard rate $HR_j(\text{per year})$, duration time of the hazard $D_j(hours)$ and the exposure time $E_j(hours)$ for the j^{th} hazard have to be defined. For each hazard, the consequences of the k accidents have to be calculated as $\sum_k(C_j^k F^k)$. This expression is called risk reduction parameters and includes the risk reduction factor C_j^k, which describes the consequence probability, that accident k occurs and the severity with the probability of fatality F^k for the k^{th} accident. Additionally, *Number of hazards*: $j = 3$, *Number of uses*: $N = 300\ a^{-1}$, *Duration time of ard j:* $D_j = 5.4\ min = 0.09\ h = 1.03E-05\ a$, *Exposure time for hazard* j: $E_j = 5.4\ min = 0.09\ h = 1.03E-05\ a$ and *Number of accidents:* $k = 9$. We compute the overall risk reduction parameter $\sum_k(C_j^k F^k)$ as 1.73E-02. With all known parameters and the assumption of 1 hazard per year, we can calculate the *IRF* caused by three hazards (H_1, H_2, H_3) as follows.

$$IRF_{H_1} = N\,[a^{-1}] \cdot\ 1\,[a^{-1}](D_1\,[a] + E_1\,[a])\left(\sum_{k=1}^{4} C_1^k F^k\right) = 5.51E-06\ a^{-1}$$

$$IRF_{H_2} = N\,[a^{-1}] \cdot\ 1\,[a^{-1}](D_2\,[a] + E_2\,[a])\left(\sum_{k=5}^{6} C_2^k F^k\right) = 1.02E-04\ a^{-1}$$

$$IRF_{H_3} = N\,[a^{-1}] \cdot\ 1\,[a^{-1}](D_3\,[a] + E_3\,[a])\left(\sum_{k=7}^{9} C_3^k F^k\right) = 7.62E-08 a^{-1}$$

The accumulative individual risk from all three hazards above becomes:

$$IRF_{H_1,H_2,H_3} = \sum_{j=1}^{3} IRF_{H_j} = 1.07E-04\ a^{-1}.$$

6.2.6.3. Risk assessment

The above calculated risks are now compared with the risk acceptance criteria. It is observed that only the Hazard H_3 has tolerable risks (below the *TIR (*1E-07 per year*))*. The other Hazards create higher risks and are not tolerable in accordance to the risk acceptance criteria. In the end, the overall risks are too high. We need to have a safety technology that should minimize the accumulative risks above to the acceptable level, say 1E-07 per year.

The HR is not known for the hazards. According to the individual risks from these hazards, we can calculate tolerable hazard rates (THR) for each hazard. For this, we take *IRF = TIR as* 1E-07 per year and compute the tolerable hazard rate (THR) as:

$$TIR = \sum_j N \cdot \left[THR_{System} \cdot \left(D_j + E_j\right) \sum_k \left(C_j^k F^k\right)\right]$$

$$1E-07\ a^{-1} = 300\ a^{-1} \cdot THR_{System} \cdot (0.09\ h + 0.09\ h)\ \cdot 1.73E-02$$

$$THR_{System} = 1.07E-07\ h^{-1}$$

If we apportion the above system level *THR* to the function level[5] we get value lower than $1.07E-07\ h^{-1}$ per function. (Here, all safety functions of the PSD technology are not discussed since the design of technology was in the conceptual phase.) Therefore, the system level *THR* calculated above will be within the discrete level that corresponds to *SIL 3* (see Figure 4.3). Therefore, SIL 3 is regarded as the safety requirement for the PSD system. In other words, the PSD system must demonstrate the lower failures than 1E-07 per hour.

The framework and consequence model offered a suitable solution for one time decision making problem. The Bayesian Networks based consequence model helped operator, supplier and independent assessor in understanding the influencing factors and their dependencies for the risk assessment of PSD system.

6.3 Summary

The objective of the work was to determine the risk-informed safety requirements for PSD system located in a megacity. The SIL requirements for the PSD were quantified. The probability values are based on real operational/infrastructural conditions and data as well as expert consultations. The models and their assessment in this work are mainly based on probability, not statistics. The framework and models presented in this chapter are useful because they have served the purpose; determination of SIL. The reliance of this study on (generic) model and data associated to the model can be a good approximation to screen the life safety risks in connection with the PSD system for a URTS in a mega city. The safety technology (PSD system) can be declared as TECHNICALLY SUITABLE provided that it fulfils the SIL 3 requirement for the specific URTS. The conclusions of the risk assessment and the safety requirements are completely based on the data and general considerations, which were site, structure and system specific. Models and their values have to be adapted to the specific environment of other PSD applications in URTS before they can be used for other risk quantification.

[5] SIL is only assigned to the safety functions of a safety technology.

CHAPTER 7: INFLUENCE DIAGRAMS BASED DECISION SUPPORT FOR RAILWAY LEVEL CROSSINGS

7.1 Introduction

In many cases, the problem of risk acceptance turns into an economic decision problem when the risks are in the so-called tolerable or ALARP region and objective is to further reduce the risks. For instance, should we introduce a safety technology if the individual risk $4 \cdot 10^{-05}$ per year is close to the risk acceptance level $5 \cdot 10^{-05}$ per year in Figure 7.1? In this situation, one may require following criteria for decision making on further reduction of risks:

- Tolerate risks if the risk reduction cost is grossly disproportionate to the benefits achieved; and
- Tolerate risks if the risk reduction cost exceeds improvement achieved.

Benefit-Cost-Analysis (BCA) and Willingness-to-Pay (WTP) are commonly applied economic based approaches in case the risks are in tolerable region. The BCA and WTP take into account the same parameters for the comparison of profitability of different safety measures. Identification of such parameters for different socio-economic and geographical conditions and assigning monetary values (to benefits and costs) of the identified parameters has complications. Detail discussion on the BCA and WTP is beyond the scope of this thesis. For further readings on the BCA and the WTP and their application to different industries readers are referred to (Evans, 2013; TD, 2000; Aoun, et al., 2012; RSSB, 2006; Evans, 2005). The WTP and BCA become difficult to apply if the parameters of the decision problem are not well known. This motivates investigations into an alternative methodology,

called LQI, see section 4.7. This chapter focuses on the justification of investment into the human safety in reference to a railway level crossing (LC). We apply Influence Diagrams (IDs), which are extensions of Bayesian Networks, to the assessment of life safety risks in railways. In IDs, problems of probabilistic inference and decision making – based on utility functions such as the LQI – can be combined and ranked and optimized. The LQI based utilities are used in the IDs to optimize the decision problem on railway level crossings. The IDs are briefly explained in sub-section 3.10.

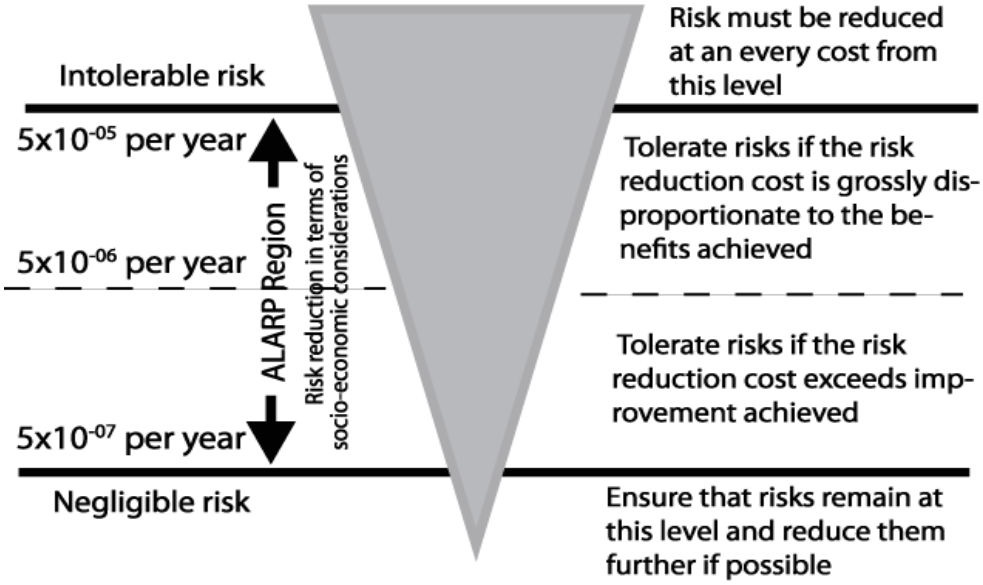


Figure 7.1: ALARP individual risk acceptance criteria for a level crossing problem

7.2 Level crossing accidents in railways

A level crossing (LC) includes conflict area, which is commonly used by rail and road traffic. Road users have to look for train before passing the technically unprotected or so-called passive LC. In contrary to passive LC, an active LC includes automatic and/or manual warnings and protections systems. For example, light signal, acoustic warning, half or full barriers are part of active LCs. It is mainly road users who make an error at the time of passing a LC. These errors can lead to severe consequences such as fatalities, injuries and damage to property. A European-level study shows that the rate per train-kilometre of fatal train

accidents related to LC between 1990 and 2009 remained unchanged, and were mainly due to errors (cause involuntary risks: to which people are exposed involuntarily to the technical system and its environment) or violations (cause voluntary risks: to which people are exposed voluntarily) from road users (Evans, 2011). The same study shows that there is an increasing trend (+0.8 % per year) of serious fatal accidents at LC between 1990 and 2009 in European railway network. Another study shows that there are on average 3.31 fatalities per 1000 LC per year (or $3.31 \cdot 10^{-03}$ per year per LC) in European railways (Evans, 2013). The latest report on railway safety performance reveals that in 2011 there were 39 fatalities in 148 LC accidents in the entire German rail network (Bundesamt, 2012).

The safety of a level crossing user can be improved sufficiently by investment. For example, installation of a safety barrier is a common approach to improve safety at a technically unprotected LC. However, the installation of safety barriers at all unprotected LC in a country is not feasible. First, it requires a lot of money. For example, in 2010 Germany had 12496 passive and 12396 active LCs (Bundesamt, 2012). Up gradation of passive LCs on so many locations requires a lot of money. Second, installation of a safety barrier at all LCs will not bring desirable benefits to society.

7.3 A case study of railway level crossing

It is necessary to estimate the present level of risks before deciding on the adoption of any safety measure. For this, we need to model, quantify and assess the causes and consequences of hazard. Therefore, a system representation is performed in terms of statistically dependent random variables such as system components and human activities. The variables and their dependence structure are shown in Figure 7.2 for hazard (from ellipse *Hazard (road and rail traffic in the danger zone)*), accidents given hazard (from ellipse *Collision between rail and road traffic*) and fatalities (from ellipse *Fatalities*) given accidents.

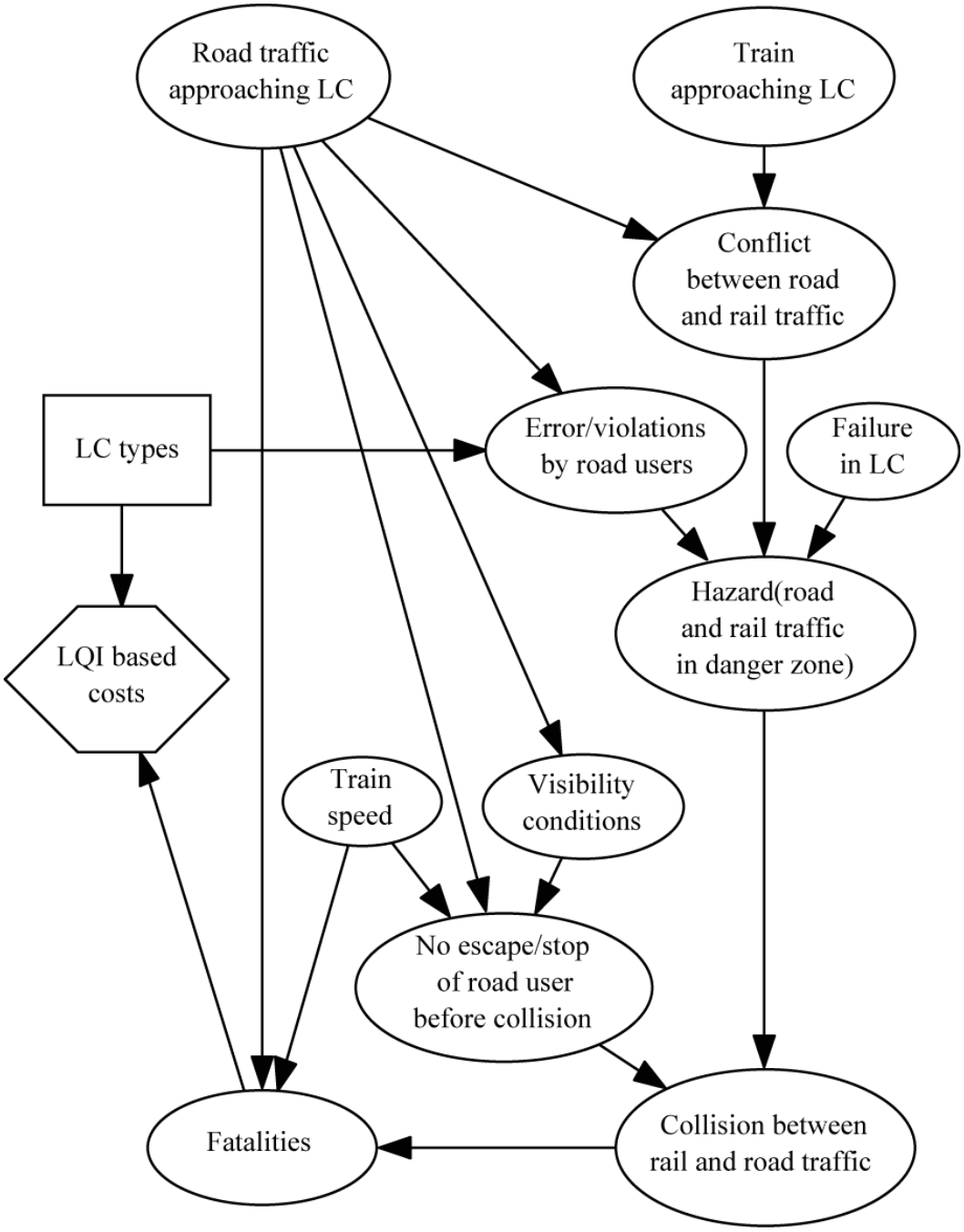


Figure 7.2: Influence diagram for decision optimization of a level crossing facility.

7.4 Characteristics of the railway level crossing under investigation

Main characteristics and assumptions of the LC system considered for the optimization are given below.

- The LC is located on a single track.
- There is one train demand at a time.
- We consider two main causes of collisions; Human errors/violations by road users and technical failures in LC. The technical failures in active level crossings are rare and considered constant ($5 \cdot 10^{-08}$ per hour) for all types of LCs.
- Train driver is not making errors/violations at LC.
- All active LCs are automatic. In other words, the operation of the active LC does not require the aid of a gateman.
- Conflict area of LC with full barrier is supervised by the additional detection technology, which further control hazards. The train will stop in case the conflict area is occupied by the road users.
- We assume that installation of half barrier and light signal technologies always allow road users to escape from the conflict area.
- We do not consider risks resulting from traffic queues after passing the LC.
- We only consider head-on collisions. It means that road traffic has very low possibility of hitting a train side. For this reason, we consider train head as an impact point. This point needs maximum 1 sec to pass the conflict area.
- Three different levels of speeds (low<60, 60<moderate<120, 120<high) are considered. The higher speed will lead to higher consequences, given the hazard as well as accidents.
- Probability values are calculated on the basis of yearly data.
- We do not consider the time dependent behaviour of a road user. In other words, road users have different error probabilities towards closing time of different level crossing barriers.

The objective of the study here is to show the application of the IDs and LQI to railway risk optimization, and not to show the detailed risk analysis of a LC. Therefore, we do not dis-

cuss the Stott-effect[6] (Stott, 1987) and influence of different level crossing characteristics (such as geometry, number of tracks, specific infrastructure and environment conditions, effects of train length) here. Such factors and their effects on LC's risk are well explained in (Schöne, 2013). Data of the road and rail traffic for a (fictitious) technically unprotected LC is presented in Table 7.1.

Table 7.1: Traffic conditions at level crossing.

Type of traffic	Arrival rate (Per hour)	Crossing time at LC (Sec.)[7]	Occupancy rate
Pedestrian	7	3.5	1
Bicyclists	6	4	1
Motorcyclists	6	4.5	1
Car	20	4.5	1.4
Truck & others	4	6	1
Train	2	1	-

We identify the causes and consequences of the hazards leading to fatalities at a LC. The causes and consequences of the hazard are shown in the IDs in Figure 7.2. Majority of LC accidents are caused by errors from road users and not from train drivers. The technical failures in active LCs are rare ($5 \cdot 10^{-08}$ per hour) and considered constant for all types of LCs. That is why the node *Failure in LC* is treated independent from the node *LC types*. Moreover, the main consequences of LC accidents are also to road users. Therefore, we neglect the life safety risks to rail users for the simplification of the study. The number of fatalities at this passive LC are 0.19 per year per $3.5 \cdot 10^{05}$ user trips (see Table 7.2) if the LC is operated for 20 hours/day and 350 days/year. If we divide the total number of user's trips by the average number of trips per user per year, we will obtain the total number of persons (N) as $7 \cdot 10^{02}$ exposed to the LC. In this way, the individual risk becomes $2.7 \cdot 10^{-04}$ per year. (In other words, probable fatality rate is approximately one in 3703 years.) Here, collision of rail with only one type of single road traffic is considered; meaning that second collision in the same moment will not occur on this LC. It is due to the fact that the traffic movement on the LC will be halted whenever any accident happens.

[6] P F Stott argued, based on Poisson distribution, that a level crossing with a moderate traffic flow has the more chances of collision. His argument is quite opposite to the linear model, which suggests that the level crossing with highest traffic has the most opportunities for collision.

[7] The crossing time also includes attention time at LC. In the case of train, one second is the crossing time of train head.

Table 7.2: Individual risks from different types of level crossings.

LC types	collisions (Per year)	Fatalities (Per year)	Individual risk of fatality (Per year)
Passive LC	0.74	0.19	$2.7 \cdot 10^{-04}$
Light signal	0.10	0.03	$4.9 \cdot 10^{-05}$
Half barrier	0.0138	0.0054	$7.7 \cdot 10^{-06}$
Full barrier	0.0035	0.002	$2.8 \cdot 10^{-06}$

Now, based on the ALARP criteria in Figure 7.1, the individual risk value $2.7 \cdot 10^{-04}$ per year is not lying within the tolerable region. Therefore, target becomes to reduce the IRF at this LC. Depending on operation, socio-economic and environmental conditions of traffic system, different types of safety measures can be adopted for the LC. In this study, we investigate the effects of following three safety measures on life safety risks:

Light signal: it is fitted with optical and acoustic warnings,

Half barrier: it is fitted with optical warnings and protects the road users with half barrier,

Full barrier: it is fitted with optical warnings and protects the road users with full barrier. In Germany, this type of level crossing protection also supervises conflict area[8]. It means that the train is not allowed to pass the LC if the conflict area is occupied by the road traffic.

There will be decrease in individual risk if one of the above safety measures is adopted for the LC. We investigate expected collisions, fatalities and individual risks for different types of LCs. Here, assumption is made that all the operation and environment conditions remain the same at the LC. In Table 7.2, the decrease in fatality rate is mainly influenced by human error probabilities (HEP). The road users have different error and visibility probabilities towards particular safety barrier. For example, HEP and visibility would be higher for a pedestrian than a car user at the same LC. For pedestrians and cyclists one should consider high risk values because they are always able to override the technical protections. These factors are considered in Figure 7.2 for all LCs.

Table 7.2 shows that one can achieve high safety level if the technically unprotected LC is replaced with one of the active LCs above. Installation of the active LCs can bring the IRF to the ALARP region in Figure 7.1. It is to mention that the long term objective of risk man-

[8] An area that can jointly be occupied by road and rail traffic is called conflict area,

agement is to bring the risks to a negligible level. Such objectives could be useful for keeping a constant eye on safety improvements in operation; however, it does not provide much help in guiding the decision makers on the utilization of available resources such as public money. To achieve this objective and solve decision problem on the particular safety improvement on the LC one requires having an additional criterion. The additional criterion should (1) aid the decision making process and (2) ensure the benefit of the investment against risk reduction. Therefore, we need to answer the following questions before taking a decision on any safety measure:

- Which safety measure is more feasible once the risks are in the ALARP region?
- How many resources society can commit towards human safety in the given risk situation?

7.5 Life quality index applied to railway level crossing risk problem

An additional criterion such as the LQI is needed to support the decision on further reduction of risks on particular LC. Data required to compute the LQI based acceptance criteria is presented in Table 7.3.

Table 7.3: Costs (in €) to calculate societal capacity to commit resource using LQI.

	Passive LC	Light Signal	Half Barrier	Full Barrier
Initial cost (IC)	$2 \cdot 10^4$	$1 \cdot 10^5$	$1.5 \cdot 10^5$	$2.1 \cdot 10^5$
Annual costs (A)	$6 \cdot 10^2$	$4 \cdot 10^3$	$7.5 \cdot 10^3$	$1.0 \cdot 10^4$
Service life(n)	30 years			
Interest rate(r)	3% per year			
German GDP (g)	$3.59 \cdot 10^4$ per person and year (in 2011)			
Yearly repayment	$9.7 \cdot 10^2$	$4.8 \cdot 10^3$	$7.3 \cdot 10^3$	$1.1 \cdot 10^4$
Yearly repayment after annual costs(YR)	$1.6 \cdot 10^3$	$8.9 \cdot 10^3$	$1.5 \cdot 10^4$	$2.1 \cdot 10^4$
Parameter β	0.8			
Parameter w	0.14			
$de/e = 13\mathrm{d}\mu$ **(μ = Fatality rate)**	-	$2.9 \cdot 10^{-3}$	$3.4 \cdot 10^{-3}$	$3.5 \cdot 10^{-3}$

How the SCCR was calculated is explained below for the LC with light signal (see column 3 in Table 7.3). The yearly repayment is calculated by using following amortization formula:

$$\text{Yearly repayment} = \frac{A \cdot r(1+r)^n}{(1+r)^{n+1} - 1} = 4.8 \cdot 10^3 €\,.$$

After adding the annual costs (like maintenance and repair costs), the total yearly repayment for the light signal LC becomes $8.9 \cdot 10^3$€. The impact of the risk reduction can be measured in terms of a change in the fatality rate once the passive LC is replaced with the light signal. It can be called as decrease in yearly fatality rate ($d\mu$) and is calculated as

$$d\mu = \frac{0.19 - 0.03}{7 \cdot 10^2} = 2.3 \cdot 10^{-4}\,.$$

It is to mention that de/e cannot directly be computed because the age-specific increase in mortality rate is not readily available. To deal with this situation, (Rackwitz, 2002; Rackwitz, 2004; Nathwani, et al., 1997) have provided a simplified formulation that are based on empirical studies. They show that a small change ($\leq 0.01\%$) in mortality rate dμ is approximately proportional to the change in life expectancy de/e. For example, there exist such approximations for Canada ($19.2\mathrm{d}\mu$), USA ($20.61\ \mathrm{d}\mu$) and Australia ($20\mathrm{d}\mu$). By utilizing Table 1 in (Rackwitz, 2002) we compute the change in life expectancy equivalent to $13d\mu$ for Germany. In this way, there will be approximately $2.9 \cdot 10^{-03}$ change in life expectancy if the light signal barrier will be installed on this LC. If we divide the total number of user's trips ($3.5 \cdot 10^{05}$) per year by the average number of trips per user ($= 2\text{trips per day} \cdot 250\text{ days per year} =$) 500 per year, we will obtain the total number of persons (N) using the particular LC as $7 \cdot 10^{02}$. Now, we have all the values to calculate the SCCR (from Eq. (4.5)) towards the light signal, which is

$$7 \cdot 10^{02} \cdot 3.59 \cdot 10^4 \cdot \frac{2.9 \cdot 10^{-3}}{0.203} = 3.6 \cdot 10^5 € \text{ per year}$$

The SCCRs towards selected safety measures are presented in Table 7.4.

Table 7.4: Societal capacity to commit resources towards different level crossings.

	Light signal	Half Barrier	Full Barrier
SCCR (€ per year)	$3.6 \cdot 10^5$	$4.26 \cdot 10^5$	$4.34 \cdot 10^5$

Next step is to assign the LQI based utility values to the different decision alternatives in the utility node of IDs in Figure 7.2. The costs associated to each type of LC are given in Table 7.5 for the case of fatalities. The symbols (+, –) in Table 7.5 means that the costs are added and/or subtracted for the total utility value of each safety measure. The costs in case of no fatality will be equivalent to the yearly repayment after annual costs ($-YR$). For instance, the cost for the passive LC will be $-1.6 \cdot 10^3$ € if no fatality occurs. The total utility value $U(.)$ of each type of LC for the case of fatality is calculated in the following way.

$$U(\text{Passive LC}) = -0.19(1.6 \cdot 10^{06}) - 1.6 \cdot 10^3 = -3.08 \cdot 10^5 €.$$

$$U(\text{Light signal}) = 3.6 \cdot 10^5 - 8.9 \cdot 10^3 - 0.03(1.6 \cdot 10^{06}) = 2.96 \cdot 10^5 €$$

$$U(\text{Half Barrier}) = 4.26 \cdot 10^5 - 1.5 \cdot 10^4 - 0.01(1.6 \cdot 10^{06}) = 4.03 \cdot 10^5 €$$

$$U(\text{Full Barrier}) = 4.34 \cdot 10^5 - 2.1 \cdot 10^4 - 0.002(1.6 \cdot 10^{06}) = 4.1 \cdot 10^5 €$$

Table 7.5: LQI based costs for different LCs when fatalities are observed.

Passive LC	Light signal	Half barrier	Full Barrier
-SVSL	+SCCR	+SCCR	+SCCR
-YR	-YR	-YR	-YR
	-SVSL	-SVSL	-SVSL

The SVSL and SCCR represent the same thing in many literatures. We use both terms in this work. The SVSL represents the money one would be spending (after the accident) to compensate the diseased family. However, the SCCR is the money society would want to spend (before the accident) to save the life. The decision making on the adoption of safety measure for this unprotected LC is explained below. One must adopt safety measure – regardless of cost – if the individual risk is equal to or greater than the intolerable limit, which

is $5 \cdot 10^{-5}$ per year in Figure 7.1. (We consider $5 \cdot 10^{-5}$ per year as target individual risk.) The individual risk on this LC is $2.74 \cdot 10^{-04}$ per year implies that one must install safety barrier. In order to select from the three available options we utilize the SCCR and expected utility criterion; because, each safety barrier have different abilities to reduce the IRF and involve different costs. The SCCR (in Table 7.4) towards a safety measure is compared with the corresponding yearly repayment after annual costs (YR (in Table 7.3)). The measure may be adopted if the SCCR of the safety measure is higher than the YR of the corresponding safety measure. Here, the SCCRs of all safety measures are higher than the YRs, which specify that all three risk reduction measures can be opted for installation.

Table 7.6: Expected utilities (€ per year) of different safety measures for LC.

	Light signal	Half Barrier	Full Barrier
Expected utility	-8850	-14800	-20700

One can argue that the SCCRs of the proposed protection strategies are close to each other (or at least not grossly disproportionate). Especially, the SCCRs of the half and full barriers are very close to each other. In this situation, the expected utilities of the safety measures can facilitate the decision making process, see Table 7.6. We obtain the optimized decision based on Eq. (3.11). The light signal LC offers maximum expected utility for this particular rail road crossing. The total expected utilities of other safety measures are much higher than the light signal. It is due to the fact that the reduction of fatalities (or individual risks) and annual costs of the three safety measures are not in proportion. Keeping in view the present level of risk, ALARP risk acceptance criteria and other socio-economic preferences of the society, one can conclude that the installation of the light signal barrier will offer higher benefits to society. Of course, decision makers can disregard the maximum expected utility criteria and opt the full barrier protection or exclusive right of the way such as a bridge or underpass if the aim is not to save money, but human life. In case of an exclusive right of way, the individual risk will reduce to a negligible level.

7.6 Summary

Life safety risks from a technically unprotected railway LC were modelled, quantified and optimized using the IDs. The risks were assessed using the ALARP criteria, which is useful in differentiating the tolerable and intolerable risks in railways. It was required to reduce the risk on the LC; because, the IRF on the LC were in the intolerable region. The societal capacity to commit resources (SCCR) based on the LQI criterion was utilized in selecting a suitable safety barrier. Expected utilities of different decision alternatives were computed using a prior decision analysis. The light signal safety barrier offered maximum expected utility for a particular LC. Thus, the optimal decision is to replace the unprotected LC, at least, with the light signal LC. We conclude that the LQI provided an additional decision support towards the adaptation of risk mitigating measures for a railway facility when the risks were in the ALARP region. In other words, it offered a rational mean to implement the ALARP. The IDs, which utilized the LQI based utilities, offered an improved framework for quantitative risk assessment, acceptability and optimality of the railway risks.

CHAPTER 8: CONCLUSIONS AND OUTLOOK

8.1 Summary and important contributions

Railway systems are rather complex and require the investigation of new methods, models, tools and techniques for modelling and analysis of their risks. This thesis mainly focuses on the application of Bayesian Networks to complex railway systems. We propose a Bayesian Networks methodology for railway risk, safety and decision support. Bayesian Networks are applied to one example application and two real-world problems. It is shown that Bayesian Networks have a number of useful characteristics that are suitable for many risk and safety problems in railways, especially those that involve dependencies, uncertainties and additional knowledge. Bayesian Networks are able to model and update information in complex railways and the problem of probabilistic inference and decision making can be combined and optimized. As a result, risk-based decision alternatives in railways can be ranked.

The **first** contribution of the thesis certainly consists of addressing some specific issues that arise in the modelling and analysis of risk-based safety in complex railways. A problem of complex railways – characterized by the presence of dependencies and uncertainties in the system – is presented in Chapter 5. These dependencies and uncertainties arose due to common causes, disjoint events, failure dependency, functional uncertainty, multistate events and additional considerations on expert knowledge in the risk models. Failing to consider such complex aspects leads to over estimation of the system risks. FTA, being a classical method, had limitations in dealing with the example application from complex railways. However, Bayesian Networks were able to handle large numbers of top events, intermediate events, uncertainties and dependencies in complex railways in concise and flexible way. No repetition of the random variables (events in the risk model) was required to introduce such dependencies and uncertainties.

The **second** contribution of this thesis consists of the computation of a number of IMs for complex systems using Bayesian Networks. It was shown that the computation of a number of IMs for a complex railway system is straightforward using standard Bayesian inference. By exploiting the use of updating properties of the Bayesian Networks, failing as well as working components of the railway system can be identified and ranked at the same time using appropriate importance measures.

The **third** contribution of this thesis consists of the application of Bayesian Networks to a real-world railway problem. A Bayesian Networks based consequence model was developed to quantify the risk reduction factor for a PSD system, installed for a URTS in a mega city. Safety integrity requirements (the so-called SILs) of the safety technology were determined using the consequence model. The Bayesian Networks based graphical representation of the consequence model helped in better understanding the risk's influencing factors and inter-and-intra dependencies among them, especially to the stakeholders (such as suppliers, operators and other system experts) who were not experts in probabilistic risk assessment. Bayesian Networks offered a suitable technique to (1) model relevant information and (2) quantify risk factors for a safety technology in railways. This consequence model was accepted by the concerned railway authorities.

The **fourth** contribution of this thesis consists of the joint treatment of ALARP and a utility based acceptability criterion and the consequence models for railways. In addition to the widely applied ALARP, MEM and MGS criteria, we applied the LQI risk acceptance criteria. IDs, which are extensions of Bayesian Networks, were utilized in the assessment of life safety risks in a railway LC problem. LQI-based utilities were used (1) to quantify the SCCR towards saving a life on the railways and (2) in the IDs to optimize the decision problems on a (fictitious) railway LC. We showed that utility based risk acceptance criteria, such as the LQI, give a useful decision aid in justifying the investment in human safety, especially in the case of a railway LC. Further, the LQI provided a means to implement the ALARP criteria.

The use of Bayesian Networks in railway risk and safety is rare. This study shows the suitability of a Bayesian Network based framework towards risk-based decision aid in railways. The suitability is shown through an example application and real world applications. Bayes-

ian Networks provided a useful tool for modelling, assessing and optimizing risks on railways.

8.2 Originality of the work

With respect to the originality of the work, it is stated that the main contributions of the thesis are concentrated in Chapters 5, 6 and 7. Most of the work presented in these chapters has not been conducted by any other researcher so far. This includes (1) the mapping of advanced aspects of fault trees into Bayesian Networks for railways and (2) the computation of the IMs for complex railways using Bayesian Networks (Chapter 5). A framework for determining the safety integrity requirements for PSD in railways is presented. A Bayesian Networks based consequence model was developed for a particular railway application (Chapter 6). An IDs based decision optimization framework was introduced for a railway LC problem. Application of the LQI, in combination with the ALARP approach, to railway risk acceptance is presented (Chapter 7).

8.3 Outlook

Throughout the present thesis, the research focus is mainly on the application of Bayesian Networks. The presented thesis addresses some parts of the issues that arise in the modelling and analysis of risk-based safety in complex railways and how they can be handled using Bayesian Networks. It should be noted that the models and their probability values in the thesis are based on particular operational/infrastructural conditions and data as well as expert consultations. Therefore, the conclusions of the risk assessment and the safety requirements are completely based on the data and general considerations, which are site, structure and system specific. Thus, models and their values have to be adapted to the specific operational environments of other similar railway applications, before they can be used for risk quantification and decision support. It implies that further studies are needed before these models and methods are applied elsewhere.

The scope of the thesis does not include the development of a universal risk management tool – a deliverable mature product – for railway operators. However, this thesis provides a foundation that can be used to develop an ID-based applied tool for railway risk management. Significant progress is possible if the developments in decision formulations for additional applications in the field of railways are made. For instance, an ID-based decision support tool for an individual railway facility, railway line or complete network can be introduced. This decision support system may include a number of hazards, a variety of influencing variables for hazards and, inter – and – intra dependencies among the hazards and uncertainties. Different decision alternatives and mitigating measures, together with their utilities, can be incorporated into the IDs. In most cases, time dependencies have great influence on the quantified risk assessment. For instance, road traffic such as pedestrians and cyclists have higher violations probabilities and possibilities, after the safety barrier has been closed at a railway LC. The errors are not time dependent; however, the violations are a function of the closing time of the barriers (and the type of barrier). In other words, the longer is the closing time of the barrier the higher the probability of violation. In this way, the change in the expected fatalities in the next time step, say after three minutes of waiting at an LC, can have an influence on risk-based decision making because the probability of an accident can increase with the passage of time due to the increased tendency of the road users to violate the safety barrier. It implies that the expected fatalities at the barriers are a function of time. The modelling of such a dynamic violation behaviour of the user is possible using dynamic Bayesian Networks. Additionally, the proposed decision support methodology can be extended beyond railway accidents or safety cases. It can be expanded to consider other hazards, such as earthquakes, fires and floods, that can have sever effects on the safety and reliability of a railway transport system. The Bayesian Networks based methodology presented in this study offers such expansion. However, the decision models should be constructed in close collaboration with actual experts and decision-makers such as transport authorities, operators and insurance companies.

BIBLIOGRAPHY

Ahmed, R., 2010. *Bayesian Network.* Rijeka: Sciyo.

Anders, E., 2008. *Ein Beitrag zur komplexen Sicherheitsbetrachtung des Bahnsystems,* TU Dresden: PhD dissertation.

Andrews, J. D. & Moss, T. R., 1993. *Reliability and risk assessment.* s.l.:John Wiley and Sons.

Aoun, R. B., Koursi, E.-M. & Lemaire, E., 2012. The cost benefit analysis of level crossing safety measures. In: *Computers in Railways Xll.* Southampton: WIT press, pp. 851-862.

Aven, T., 2008. *Risk analysis.* West Sussex: John Wiley & Sons.

Aven, T., 2011. *QUANTITATIVE RISK ASSESSMENT: The Scientific Platform.* New York: Cambridge University Press.

Aven, T., 2012. Foundational Issues in Risk Assessment and Risk Management. *Risk Analysis,* 32(10), pp. 1647-1655.

Bearfield, G. & Marsh, D. W. R., 2005. *Generalising Event Trees using Bayesian Networks with a Case Study of Train Derailment.* s.l., LNCS 3688, pp. 52-66.

Benjamin, J. & Cornell, C., 1970. *Probability, Statistics, and Decisions for Civil Engineers.* New York: McGraw-Hill.

Bensi, M., 2010. *A Bayesian Network Methodology for Infrastructure Seismic Risk Assessment and Decision Support,* UC Berkeley: PhD thesis.

Bensi, M., Der Kiureghian, A. & Straub, D., 2011. *A Bayesian Network Methodology for Infrastructure Seismic Risk Assessment and Decision Support,* College of Engineering, University of California, Berkeley: PEER Report 2011/02, Pacific Earthquake Engineering Research Center.

Bernardo, J. M. & Smith, A. F. M., 2000. *Bayesian Theory.* West Sussex: JOHN WILEY & SONS, LTD.

Beugin, J., Renaux, D. & Cauffriez, L., 2007. A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems. *Reliability Engineering & System Safety,* Volume 92, pp. 1686-1700.

Birnbaum, Z. W., 1969. *On the importance of different components in a multi-component system. In Multivariable Analysis II, P.R. Kor-ishnaiah, Ed,* New York,NY: Academic Press.

Bobbio, A., Portinale, L., Minichino, M. & Ciancamerla, E., 2001. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering and Systen Safety 71,* pp. 249-260.

Borgonovo, E. & Apostolakis, G., 2001. A new importance measure for risk-informed decision making. *Reliability Engineering & System Safety,* 72(2), pp. 193-212.

Borgonovo, E., Apostolakis, G. E., Tarantola, S. & Saltelli, A., 2003. Comparison of global sensitivity analysis techniques and importance measures in PSA. *Reliability Engineering & System Safety,79(2),* pp. 175-185.

Borgonovo, E. & Smith, C., 2011. A study of Interactions in the Risk Assessment of Complex Engineering Systems: An Application to Space PSA. *Operations Research,* 59(6), pp. 1461-1476.

Bowles, J. B., 2002. Commentary-Caution: Constant Failure-Rate Models May be Hazardous to Your Design. *IEEE TRANSACTIONS ON RELIABILITY ,* 51(3), pp. 375-377.

Braband, J., 2001. A Practical Guide to Safety Analysis Methods. *SIGNAL+DRAHT,* 93(9), pp. 41-44.

Braband, J., 2010. On the Justification of a Risk Matrix for Technical Systems in European Railways . In: E. Schneider & G. Tarnai, eds. *FORMS/FORMAT* . Heidelberg: Springer, pp. 185-192.

Braband, J. et al., 2006. *The CENELEC-Standards regarding Functional Safety,* Hamburg: Eurailpress.

Braband, J. & Lennartz, K., 2000. Risk-oriented apportionment of safety integrity requirements-an example. *SIGNAL+DRAHT,* pp. 35-39.

Bucher, C., 2009. *Computational Analysis of Randomness in Structural Mechanics.* Structures and Infrastructures Book Series, Vol. 3 ed. Leiden: CRC Press.

Bundesamt, S., 2012. *Betriebsdaten des Schienenverkehrs 2011,* Wiesbaden: Statistisches Bundesamt.

CENELEC, 2012. *European Committee For Electronic Standardization.* [Online] Available at: http://www.cenelec.eu/index.html [Accessed 06 2013].

Chen, S., Ho, T. & Mao, B., 2007. *Reliability evaluations of railway power supplies by fault-tree analysis.* doi: 10.1049/iet-epa:20060244, s.n., pp. 161-172.

Cheok, M. C., Parry, G. W. & Sherry, R. R., 1998. Use of importance measures in risk-informed regulatory applications. *Reliability Engineering and System Safety ,* Volume 60, pp. 213-226.

Darwiche, A., 2010. What are Bayesian networks and why are their applications growing across all fields?. *Communications of the ACM,* 53(12), pp. 80-90.

Der Kiureghian, A., 2005. First- and second-order reliability methods. In: E. N. e. al., ed. *Chapter 14, in Engineering design reliability handbook.* Boca Raton: CRC.

Dhillon, B., 2007. *Human Reliability and Error in Transportation Systems.* London: Springer.

Dhillon, B., 2011. *Transportaiton Systems Reliability and Safety.* 1st ed. Boca Raton: CRC.

ERA, 2013. *Intermediate report on the development of railway safety in the European Union.* [Online] Available at: http://www.era.europa.eu/Core-Activities/Safety/Safety-Performance/Pages/Safety-Performance-Report.aspx [Accessed 07 06 2013].

Ericson, C. A., 2005. *Hazard Analysis Techniques for System Safety.* New Jersey: John Wiley & Sons.

EU, 2012. *EU TRANSPORT IN FIGURES: STATISTICAL POCKETBOOK,* Luxembourg: European Union.

Evans, A., 2011. Fatal Train Accidents On Europe`s Railways: 1980-2009. *Accident Analysis and Prevention,* 43(1(391-401)).

Evans, A. W., 2003. *Estimating transport fatality risk from past accident data.* London: Elsevier.

Evans, A. W., 2005. Railway Risks, Safety Values and Safety Costs. *Transport, part of the Proceedings of the Institution of Civil Engineers,* 158(TRI), pp. 3-9.

Evans, A. W., 2013. THE ECONOMICS OF RAILWAY SAFETY. *Research in Transport Economics,* p. 10.1016/j.retrec.2012.12.003.

Faber, M. H., 2012. *Statistics and Probability Theory: In Pursuit of Engineering Decision Support.* Topics in Safety, Risk, Reliability and Quality, Vol. 18 ed. s.l.:Springer.

Faber, M. H., Straub, D., Montes-Iturrizaga, R. & Heredia-Zavoni, E., 2012. Risk Assessment for Design of FPSO Systems. Part I: Generic Models and Acceptance Criteria. *Marine Structures,* 28(1), pp. 120-133.

Flammini, F., Gglione, A., mazzocca, N. & Pragliola, C., 2009. Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures. In: R. S. a. S. G. (Eds.), ed. *CRITIS 2008.* Berlin Heidelberg: Springer-Verlag, pp. 180-189.

Ford, R., 2001. Modern Railways. *The Forgotten Driver*, January, pp. 45-48.

Fussell, B., 1975. How to hand-calculate system reliability characteristics. *IEEE Trans. on Reliability,* p. 24(3).

Gelman, A., Carlin, J. B., Stern, H. S. & Rubin, D. B., 2009. *Bayesian Data Analysis.* 2nd ed. Florida: CRC .

Hanea, D. & Ale, B., 2009(b). Risk of human fatalities in building fires: A decision tool using Bayesian Networks. *Fire Safety,* Volume 44(5), pp. 704-710.

Hanea, D. M., 2009(a). *Human Risk of Fire: Building a decision support tool using Bayesian Networks,* TU Delft: PhD thesis.

Heredia-Zavoni, E., Montes-Iturrizaga, R., Faber, M. & Straub, D., 2012. Risk assessment for structural design criteria of FPSO systems. Part II: Consequence models and applications to determination of target reliabilities. *Marine Structures,* Volume 28, pp. 50-66.

Holicky, M. & Diamantidis, D., 2008. Optimization of Road Tunnel Safety. *Beton- und Stahlbetonbau, Special Edition,* Issue 103.

Holmgren, M., 2005. Maintenance-related losses at the Swedish rail. *Quality in Maintenance Engineering,* 11(1), pp. 5-18.

IEC 61508, 2000. *Functional safety of electrical/electronic/programmable electronic safety-related systems(IEC 61508-1 to 7),* Geneva: IEC(International Electronical Commission).

IRSC, I. R. S. C., 2008. *Rail Optimization and Safety Analysis.* [Online] Available at: http://www.intlrailsafety.com/DenverConference2008.html [Accessed 15 January 2010].

Jensen, F. V. & Nielsen, T. D., 2007. *Bayesian Networks and Decision Graphs.* Berlin: Springer.

Kalos, M. H. & Whitlock, P., 2004. *Monte Carlo Methods.* 1st ed. VCH-Verlag: Wiley.

Kang, D., Kim, K. & Ha, J., 2002. Importance Analysis of In-Service Testing Components for Ulchin Unit 3 Using Risk-Informed In-Service Testing Approach. *Journal of the Korean Nuclear Society,* 33(4), pp. 331-343.

Kerbs, H., Trung, B. L., Koursi, E. M. E. & Firpo, P., 2000. Minimale Endogene Mortalität- ein universelles Sicherheitskriterium. *ETR - Eisenbahntechnische Rundschau*, 49(12), pp. 816-821.

Khakzad, N., Khan, F. & Amyotte, P., 2011. Safety Analysis in Process Facilities: Comparison of Fault Tree and Bayesian Network Approaches. *Reliability Engineering and System Safety,* p. doi:10.1016/j.ress.2011.03.012.

Khakzad, N., Khan, F. & Amyotte, P., 2013. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Safety and Environmental Protection,* 91(1-2), pp. 46-53.

Kiureghian, A. D., 2005. First- and Second-Order Reliability Methods. In: E. Nikilaidis, D. M. Ghiocel & S. Singhal, eds. *Engineering Design Reliability Handbook.* s.l.:CRC Press, p. Chapter 14.

Kjaerulff, U. B. & Madsen, A. L., 2007. *Bayesian Networks and Influence Diagrams: A Guide to Construction and Analysis.* New York: Springer.

Koller, D. & Friedman, N., 2009. *Probabilistic Graphical Models-Principles and Techniques.* ISBN-10: 0-262-01319-3: MIT Press.

Kottegoda, N. T. & Rosso, R., 2008. *APPLIED STATISTICS FOR CIVIL AND ENVIRONMENTAL ENGINEERS.* West Sussex: Blackwell Publishing Ltd.

Lampis, M. & Andrews, J. D., 2009. Bayesian Belief Networks for System Fault Diagnostics. *Quality and Reliability Engineering International,* pp. 409-426.

Lentz, P., 2007. *Acceptablity of civil engineering decisions involving human consequences, PhD thesis,* s.l.: lehrstuhl für Massivbau, Technische Universität München.

Lindley, D., 1982a. *The Bayesian approach to statistics:In Some Recent Advances in Statistics.* London: Academic Press.

Lu, Y., Li, Q. & Hinze, J., 2011. Subway System Safety Risk Analysis Based on Bayesian Network. *Computational Risk Management,* DOI: 10.1007/978-3-642-15243-6_25(Part 5), pp. 219-227.

Mahboob, Q., Kunze, M., Radczimanowski, G. & Trinckauf, J., 2013. *RISK-INFORMED SAFETY REQUIREMENT OF PLATFORM SCREEN DOORS FOR URBAN RAIL TRANSIT SYSTEM IN A MEGA CITY.* Amsterdam, ESREL 2013 conference proceedings.

Mahboob, Q., Kunze, M., Trinckauf, J. & Maschek, U., 2012(a). *A Flexible and Concise Framework for Hazard Quantification: An Example from Railway Signalling System.* Proceedings of the QR2MSE, Chengdu, IEEE Xplore.

Mahboob, Q., Schoene, E., Kunze, E. & Trinckauf, J., 2012(b). *Application of importance measures to transport industry: Computation using Bayesian networks and Fault Tree Analysis.* Chengdu, IEEE Xplore.

Mahboob, Q. et al., 2012(c). REPRESENTING ADVANCED ASPECTS OF FAULT TREES INTO BAYESIAN NETWORKS - MODELLING SAFETY IN COMPLEX RAILWAY SYSTEMS. In: 9781622764365, ed. *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference.* Helsinki, Finland: Curran Associates, Inc., pp. 711-718.

Mahboob, Q. et al., 2012(d). COMPUTATION OF COMPONENT IMPORTANCE MEASURES FOR RELIABILITY OF COMPLEX SYSTEMS. In: E. E. K. F. T. B. Cengiz Kahraman, ed. *Uncertainty modeling in knowledge engineering and decision making.* edited by Kahraman, C. et al. ed. FLINS 2012 proceedings, Istanbul: World Scientific Publishing, pp. 1051-1057.

Marsh, W. & Bearfield, G., 2007. *Representing Parametrized Fault Trees Using Bayesian Networks.* Heidelberg, Springer, pp. 120-1333.

Maschek, U., 2012. *SICHERUNG DES SCHIENENVERKEHRS: GRUNDLAGEN UND PLANUNG DER LEIT- UND SICHERUNGSTECHNIK.* ISBN: 978-3-8348-1020-5 ed. Wiesbaden: Springer Vieweg.

Melchers, R., 2001. On the ALARP approach to risk management. *Reliability Engineering and System Safety,* 71(2), pp. 201-208.

Misra, K. B., 2008. *THE HANDBOOK OF PERFORMABILITY ENGINEERING.* London: Springer-verlag.

Modarres, M., 2008. Probabilistic Risk Assessment. In: K. B. (. Misra, ed. *Handbook of Performability Engineering.* s.l.:Springer, pp. 699-718.

Mohaghegh, Z., Kazemi, R. & Mosleh, A., 2009. Incorporating Organizational Factors into Probabilistic Risk Assessment (PRA) of Complex Socio-technical Systems: A Hybrid Technique Formalization. *Reliability Engineering & System Safety,* 94(5), pp. 1000-1018.

Mokkapati, C., 2004. *A practical risk and safety assesment methodology for safety-critical systems.* Nashville, Proceedings of the AREMA 2004 Annual Conferences.

Murphy, K. P., 2002. *Dynamic Bayesian Networks: Representation, Inference and Learning,* UC Berkely: PhD thesis.

NASA, 2002. *Fault Tree Handbook with Aerospace Applications.* Washington, DC: NASA Office of Safety and Mission Assurance.

Nathwani, J. S., Lind, N. & Pandey, M., 1997. *Affordable safety by choice: the life quality method.* Waterloo, Canada: Institute for Risk Research, University of Waterloo.

Nelson, D. & O'Neil, K., 2000. Commuter rail-service reliability: On time performance and causes of delays. *Transportation Research Board,* Issue 1704, pp. 42-50.

Nishijima, K., 2012. *Lecture notes (Summer semester 2012): Engineering Risk and Decision Analysis,* Lyngby: CERDA: Technical University of Denmark.

Oukhellou, L., Côme, E., Bouillaut, L. & Aknin, P., 2008. Combined use of sensor data and structural knowledge processed by Bayesian network: Application to a railway diagnosis aid scheme. *Transportation Research Part C: Emerging Technologies,Volume 16, Issue 6,* pp. 755-767 .

Podofillini, L., Zio, E. & Vatn, J., 2006. Risk-informed optimisation of railway tracks inspection and maintenance procedures.. *Reliability Engineering and System Safety,* 91(1), pp. 20-35.

Prescott, D. & Andrews, J., 2010. *Component Importance Measures To Identify Contributions To System Failure For Aircraft Which Dispatch With Known Faults.* Taylor Francis. 675-682, ESREL 2010.

Puettner, R. & Geisler, M., 2008. *ROSA - Rail Optimization Safety Analysis.* Denver, IRSC.

Rackwitz, R., 2002. Optimization and risk acceptability based on the Life Quality Index. *Structural Safety,* Issue 24, pp. 297-331.

Rackwitz, R., 2004. Optimal and Acceptable technical Facilities Involving Risks. *Risk Analysis,* 24(3), pp. 675-695.

Rackwitz, R., 2008. *The Philosophy Behind the Life Quality Index and Empirical Verification,* Joint Committee of Structural Safety (JCSS): Basic Documents on Risk Assessment in Engineering, Document # 4.

Rashidi, T. H. & Mohammadian, A., 2011. Parametric Hazard Functions: Overview. *Transportation Research Record: Journal of the Transportation Research Board,* Issue 2230, pp. 48-57.

Rausand, M. & Hoyland, A., 2004. *System Reliability Theory: Models, Statistical Methods, and Applications.* Hoboken: John Wiley & Sons.

Recht, J., 1966. *Failure modes and Effects Analysis,*: National Safety Council.

Ross, S. M., 1997. *Introduction to Probability Models.* 6th ed. CA: ACADEMIC PRESS.

Rouvroye, J. L. & van den Bliek, E. G., 2002. Comparing safety analysis techniques. *Reliability Engineering & System Safety,* Volume 75, pp. 289-294.

RS, L., 2001. *Risk Profile Bulletin:Profile of Safety Risk on Railtrack PLC- Controlled Infrastructure. Issue 2,* London: RS, London.

RSSB, 2006. *SELCAT: D4 - Report on Cost Benefit Analysis methods for level crossings, Safer European Level Crossing Appraisal and Technology,* http://www.iva.ing.tu-

bs.de/levelcrossing/selcat/lcDocuments/867-867-26_SELCAT-D4.pdf: Rail Safety and Standards Board (RSSB).
RSSB, 2011. Safety Risk Model: Risk Profile Bulletin. *Version 7*, August.
Rubinstein, r. Y. & Kroese, D. P., 2007. *Simulation and the Monte Carlo Method.* Second ed.:Wiley .
Russell, S. & Norvig, P., 2010. *Artificial Intelligence: A Modern Approach.* New Jersey: Prentice Hall.
Russel, S. & Norvig, P., 2010. *Artificial Intelligence: A Modern Approach.* 3rd ed. New jersey: PEARSON.
Sapoznikov, V., Sapoznikov, V., Anders, E. & Trinckauf, J., 2009. Safety and Reliability in Signalling Systems. In: G. Theeg & S. Vlasenko, eds. *Railway Signalling and Interlocking.* Hamburg: Eurail press, pp. 24-38.
Schöne, E., 2013. *Ein risikobasiertes Verfahren zur Sicherheitsbeurteilung von Bahnübergängen,* TU Dresden: PhD Thesis.
Singpurwalla, N. D., 2006. *Reliability and Risk.* West Sussex: John Wiley & Sons Ltd.
Si, S., Liu, G., Cai, Z. & Xia, P., 2011. *Using Bayesian Networks and Importance Measures to Indentify Tumour Markers for Breast Cancer.* Singapore.
Sotera, L., 2006. *Developing a location specific risk model for Irish rail.* [Online] Available at: http://www.sotera.co.uk/pdf/Location%20specific%20risk%20model.pdf [Accessed 9 February 2010].
Spackova, O. & Straub, D., 2013. Dynamic Bayesian Network for Probabilistic Modeling of Tunnel Excavation Processes. *COMPUTER-AIDED CIVIL AND INFRASTRUCTURE ENGINEERING,* 28(1), pp. 1-21.
Spiegel, 2013. *'I've Derailed!': Excess Speed Suspected in Spanish Rail Disaster.* [Online] Available at: http://www.spiegel.de/international/europe/investigation-focuses-on-speed-as-possible-cause-of-spain-rail-crash-a-913195.html [Accessed 26 07 2013].
Stewart, M. G. & Melchers, R. E., 1997. *Probabilistic Risk Assessment of Engineering Systems.* London: Chapman & Hall.
Stott, P., 1987. *Automatic Level Crossing-A review of safety,* London.
Straub, D., 2005. *Natural hazards risk assessment using Bayesian networks,* (Proc. ICOSSAR 05, Rome): Safety and Reliability of Engineering Systems and Structures, Augusti et al. (eds), Millpress .
Straub, D., 2009. Stochastic modeling of deterioration processes through dynamic Bayesian networks. *Journal of Engineering Mechanics,* 135(10), pp. 1089-1099.
Straub, D., 2011. *Lectures on Risk Analysis,* TU München: Engineering Risk Analysis Group.
Straub, D. & Kiureghian, A. D., 2010. Bayesian Networks Enhanced with Structural Reliability Methods.Part B: Application. *Journal of Engineering Mechanics,* 36(10), pp. 1259-1270 .
Straub, D., Lentz, L., Papaioannou, I. & Rackwitz, R., 2011. *Life Quality Index for Assessing Risk Acceptance in Geotechnical.* München, s.n., pp. 37-45.
TD, 2000. *Transport Division, EVALUATION OF COST-EFFECTIVE SYSTEMS FOR RAILWAY LEVEL-CROSSING PROTECTION.* [Online] Available at: http://www.unescap.org/ttdw/Publications/TIS_pubs/pub_2088/level-

crossing-fulltext.pdf
[Accessed January 2013].
Trinckauf, J., 2013(b). Visionen und Aussichten in der Bahnsicherungstechnik. *Deine Bahn,* Issue 1.
Trinckuaf, J., 2013(a). About the Assessor. *Signal+Draht,* Issue 3.
U.S.N.R.C, 2012. *Regulatory Guide 1.174.* [Online] Available at: http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/rg/01-174/
[Accessed 10 11 2012].
Vatn, J. & Svee, H., 2002. *A Risk Based Approach to Determine Ultrasonic Inspection Frequencies in Railway Applications.* Madrid, 6th Proceedings of the 22nd ESReDA Seminar.
Vesely, W., Goldberg, F., Roberts, N. & Haasl, D., 1981. *Fault Tree Handbook.* Washington, D.C: U.S.N.R.C.
Xing, L., 2004. *Maintenance-Oriented Fault Tree Analysis of Component Importance.* Los Angeles, CA, USA, pp. 534-539.
Xing, L. & Amari, S. V., 2008. Fault Tree Analysis. In: *Handbook of Performability Engineering.* London: Springer, pp. 595-620.
Zhou, Z., Jin, G., Dong, D. & Zhou, J., 2006. *Reliability analysis of multistate systems based on Bayesian networks.* Postdam.
Zio, E., 2007. *INTRODUCTION TO THE BASICS OF RELIABILITY AND RISK ANALYSIS: Sries on Quality, Reliability, and Engineering Statistics.* Vol. 13 ed. sINGAPORE: World Scientific.
Zio, E., 2009. *COMPUTATIONAL METHODS IN RELIABILITY AND RISK ANALYSIS.* Series on Quality, Reliability and Engineering Statistics, Vol. 14 ed. Singapore: World Scientific Publishing.
Zio, E., 2013. *The Monte Carlo Simulation for System Reliability and Risk Analysis.* Springer Series in Reliability Engineering:Springer.

APPENDIX 1: **Preliminary hazard analysis of platform screen door system.**

ID	Sub-system	Hazard description	Hazard cause(s)	Risk reduction measures	Hazard resolution status
1	signalling	train departs too early while PSD are opened	failure in signalling	Within signalling system solutions and back-up system	closed
2	signalling	accident: train arrives while another train is at platform	failure in signalling	Within signalling system solutions and back-up system	closed
3	signalling	train moves to station while PSD are opened	failure in signalling	Within signalling system solutions and back-up system	closed
4	train	train arrives at wrong position (half door)	imprecise train control and track conditions	Emergency Exit, Emergency release	closed
5	train door	train departs too early while train door is open and PSD closed	failure in train door control	Emergency Exit, Emergency release	closed
6	train	train is too short, train arrives at wrong position (1 car)	imprecise train control, failure, wrong train configuration	Emergency Exit, Emergency release, track free detection	closed
7	train	fire/external event in train stopping at platform	fire, terrorism, etc.	Emergency Exit, Emergency release	closed
8	train	fire/external event in train stopping near to platform	fire, terrorism, etc.	Emergency Exit, Emergency release	closed
9	train door	train door opens while train is moving/PSD closed	failure in train door control	Emergency Exit, Emergency release	closed
10	train door	train door does not open/is locked, PSD open, person in danger zone	failure in train door/train door control	Space between doors, PSD Obstacle detection	closed
11	train door	train door opens after PSD closed; person trapped	emergency exit, failure in train door/train door control	As given in event tree # 3	in progress
12	PSD	PSD opens before train arrives at platform	failure in PSD system or signalling interface	As given in event tree analysis # 1	in progress
13	PSD	PSD does not open while train deboards at platform	failure in PSD system or signalling interface	PSD Obstacle detection, Emergency Exit, Emergency release	closed
14	PSD	PSD remains opened and train departs	failure in PSD system or signalling interface	As given in event tree analysis # 2	in progress
15	PSD	PSD opens too late and pushes person away from door with rubber elements	bad door drive conditions	Emergency Exit, Emergency release	closed
16	PSD	PSD closes with high force/without reversing	failure of door drive/reversing	obstacle protection, regular door maintenance	closed
17	Power supply	Complete shutdown of power supply	Failure in source and supply	Back-up system for power supply is provided	Closed

Proof-Reading-Service.com
PhD theses, journal papers, books and other professional documents

Proof-Reading-Service.com Ltd, Devonshire Business Centre, Works Road, Letchworth Garden City, Hertfordshire, SG6 1GJ, United Kingdom
Office phone: +44(0)20 31 500 431
E-mail: enquiries@proof-reading-service.com
Internet: http://www.proof-reading-service.com
VAT registration number: 911 4788 21
Company registration number: 8391405

06 November 2013

To whom it may concern,

RE: Proof-Reading-Service.com Editorial Certification

This is to confirm that the document described below has been submitted to Proof-Reading-Service.com for editing and proofreading.

We certify that the editor has corrected the document, ensured consistency of the spelling, grammar and punctuation, and checked the format of the sub-headings, bibliographical references, tables, figures etc. The editor has further checked that the document is formatted according to the style guide supplied by the author. If no style guide was supplied, the editor has corrected the references in accordance with the style that appeared to be prevalent in the document and imposed internal consistency, at least, on the format.

It is up to the author to accept, reject or respond to any changes, corrections, suggestions and recommendations made by the editor. This often involves the need to add or complete bibliographical references and respond to any comments made by the editor, in particular regarding clarification of the text or the need for further information or explanation.

We are one of the largest proofreading and editing services worldwide for research documents, covering all academic areas including Engineering, Medicine, Physical and Biological Sciences, Social Sciences, Economics, Law, Management and the Humanities. All our editors are native English speakers and educated at least to Master's degree level (many hold a PhD) with extensive university and scientific editorial experience.

Document title:	**A Bayesian Network Methodology for Railway Risk, Safety and Decision Support**
Author(s):	**Qamar Mahboob**
Format:	**British English**
Style guide:	**Harvard**
Particular comments:	**None**