Risk and Safety in Engineering Processes

Risk and Safety in Engineering Processes

By

Ivan Lucic

Cambridge Scholars Publishing

Risk and Safety in Engineering Processes

By Dr. Ivan Lucic

This book first published 2015

Cambridge Scholars Publishing

Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN (10): 1-4438-7077-3
ISBN (13): 978-1-4438-7077-1

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

CONTENTS

LIST OF FIGURES

LIST OF TABLES

Foreword

It has been my pleasure to have known and worked with Ivan for the last five years. His passion for work and his work ethic towards making potentially complex and complicated procedures easier to understand, not only for professionals in the risk and safety field, but also to the lay person, is motivational.

A lot of research went into the production of this book, looking at how risk and safety was managed in the past, and where either additional clarity or changes to the processes were required. The output from this research, and this book, has been developed into the Engineering Safety and Assurance Case (ESAC) that has been used on London Underground on it's last two major projects over 8 years, the Victoria Line Upgrade programme (£1.5 billion cost) and the Sub-surface Upgrade Programme (approx £5 billion cost).

The ESAC combines all the arguments and evidence required to prove that the Engineering Safety, Reliability, Availability, Maintainability, Operability and performance of the "changed Railway" is fit for purpose and meets the client's requirements. It also ensures that the appropriate amount of analysis and work is undertaken dependent on the type of change.

To date, because of the structure of the ESAC and the training Ivan has given to project / programme staff to ensure they know the when, why and what of the process, every ESAC has been delivered on time and been accepted first time every time.

This is all credit to Ivan and the motivation he gives to his staff.

Jonathan Harding
MSc, BSc, CEng, CPhys, MInstP, MIEnvSc

PREFACE

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

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

Four projects were utilised as case studies for the evaluation of existing methodologies, processes, and initial development. Later, this book describes the methodology adopted in support of the development of the System Safety Case and its structure.

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

The trial was successful and the new framework, referred to as the Engineering Safety and Assurance Case Management Process, has now been implemented across the London Underground Capital Programmes Directory.

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

ACKNOWLEDGMENTS

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

I am immensely thankful to friends and colleagues from my team in LU who work with me, patiently enhancing my understanding and stubbornly helping me to implement my ideas on very challenging projects. So thank you, very much, Jon Harding, Xenophon Christodoulou, Roger Short, Dr. Bruce Elliott, Ian Shannon, Dr. Lucy Regan, Peter Stanley, Rob Jones, Mukesh Sharma, Michael Mangroo, Mike Lester, Ian Innes, Paul Lawless, Tim Ballantyne, Chi Wang and Dr. Josh Ahmed.

A very special thank-you, to Ricardo Hetherington, a very good friend of mine, and the editor of the book.

CHAPTER ONE

INTRODUCTION

1.1 Problem area

In engineering problems, detailed analyses of risk and its attributes can lead to significant benefits in safety performance along with savings in time and money.

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

However, none of these amount to an integrated framework for the analysis and management of a system's safety risk .

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

Furthermore, none of the processes depicted in the available literature provide any guidance in relation to the monitoring of changes to the system during its lifecycle, and the control of the impact of that change on the safety performance of the system. These are just some of the shortcomings of the existing processes and guidelines.

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

1.2 Objectives and Aim of the book

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

History demonstrates that safety failures can have significant societal costs, life or health, monetary and environmental. Again, history shows that most, if not all, accidents are avoidable.

Thus, society and legislation dictate that we all have a ‘Duty of Care’ to the following groups:

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

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

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

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

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

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

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

These principles are:

1 Systematic Approach to defining the problem space;
2 Holistic approach to the analysis and assessment;
3 Necessity of extensive use of Domain Specific Expertise.

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

In summary, the result of the research project, reported in this book, is a decision supporting methodology, that was used as part of making and managing decisions involving system safety risk, and in the development of the safety cases on one of the most complex railway projects in the UK, the upgrade of London Underground’s Victoria Line (Lucic and Short, 2007) and Subsurface Lines (Metropolitan, District, Circle and Hammersmith & City and East London).

1.3 Structure of this book

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

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

The First chapter outlines the aim, objectives and scope of the book, and presents the structure that we will follow. It also presents the more important definitions that will be used later on.

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

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

The Fourth chapter outlines the initial applied research areas, and presents the findings of the early development of the methodology. Also described are four real life projects that have been used as a vehicle for initial development and testing.

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

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

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

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

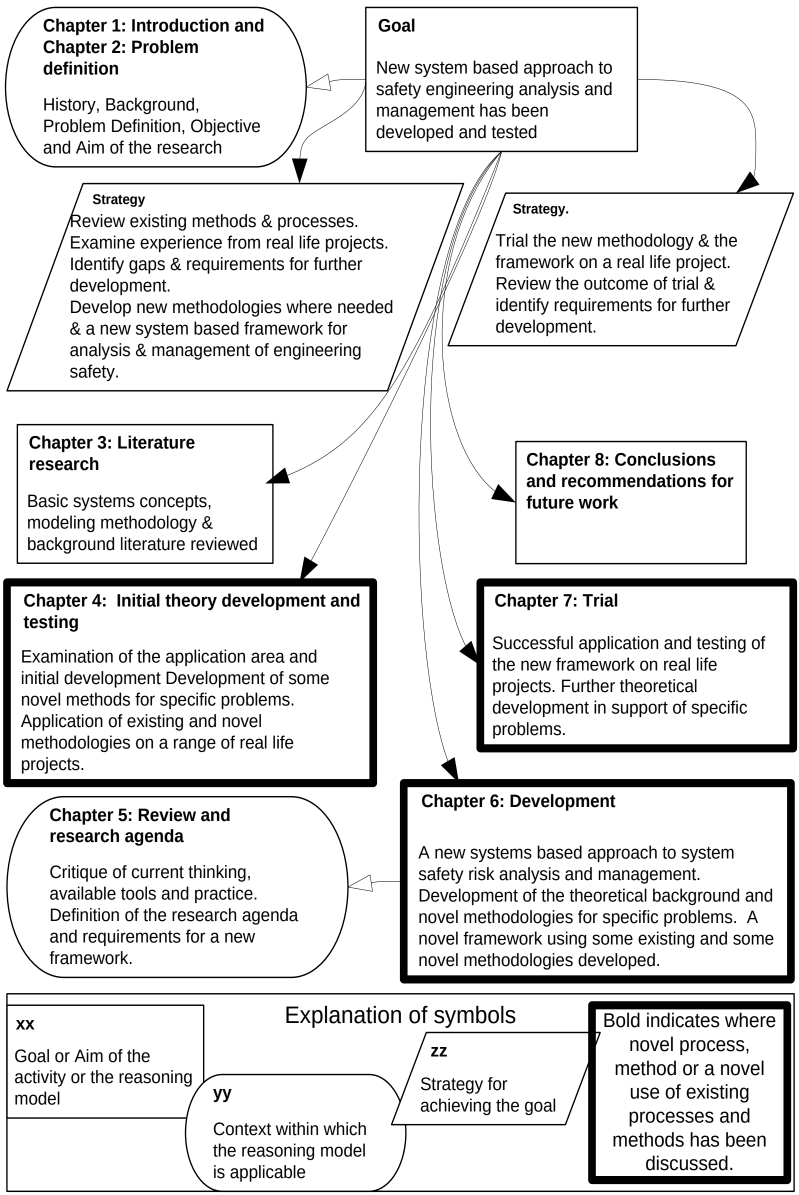

Figure 1-1: Overall Structure of the book

1.4 Definitions

The following are key definitions of terms used throughout the book:

1. A System is an interconnection, an organisation of objects that is embedded in a given environment (Karcanias, 2003). The system is the sum of all constituent parts working together within a given environment to achieve a given purpose within a given time period. The totality of the system is a matter of perspective. It is not a fixed term, but can be defined arbitrarily;
2. System Conceptualisation is a process of the development of the internal (constituent parts and their connections) and external (environment) system specification. A conceptual model should reflect knowledge about the application domain rather than about the implementation of the system (Milloti, 2004);
3. A Hazard is defined as an object, act or condition that is likely to lead to an accident;
4. An Accident is an unplanned, unintended event, entailing loss;
5. A Consequence is the outcome of a hazard;
6. A Loss is defined as an undesirable, detrimental effect of an accident;
7. An opposite of the hazard is an Opportunity. This is an object, act or condition likely to lead to a gain;
8. A Gain is a desirable effect of the opportunity;
9. A Risk is a forecast for a future accident of a certain severity. An opposite of risk is reward;
10. A Risk Profile is a multi-dimensional presentation of forecasts for future accidents, of certain severities, for a system. Additional dimensions introduced, may be time, space or some other relevant variable parameters.

1.5 Acronyms and Abbreviations

Acronym	Definition
AC	Alternating Current
ACC	Area Control Centre
AGC	Agreement on Main International Railway Lines standard (English translation)
AGTC	Agreement on Important International Combined Transport Lines and Related Installations (English translation)
ALARP	As Low As Reasonably Practicable

Acronym	Definition
ALF	Algorithm File
ATO	Automatic Train Operation
ATP	Automatic Train Protection
AWS	Automatic Warning System
BBN	Bayesian Belief Network
BS	British Standards
BT	Bombardier Transportation
BTLUP	Bombardier Transportation London Underground Projects
CCS	Control Command and Signalling
CCTV	Closed Circuit Television
CENELEC	European Committee for Electrotechnical Standardisation (English translation)
CIS	Customer Information Systems
CM	Coded Manual (mode of operation of the new train)
CRMS	Cable Route Management System
CSA	Change Safety Analysis
CSDE	Correct Side Door Enable
CSP	Current Safety Performance
CSPSSL	Current Safety Performance SubSurface Lines
CSPVL	Current Safety Performance Victoria Line
DC	Direct Current
DRACAS	Defect Reporting, Analysis and Corrective Action System
DTG-R	Distance To Go – Radio (signalling system)
ECB	Engineering Change Board
ECR	Engineering Change Request
EDF	Électricité de France (Energy Provider company)
EEPL	EDF Energy Powerlink Limited
ELLCCR	Extra Low Loss Conductor Rail
EMC	Electro-Magnetic Compatibility
EMI	Electro-Magnetic Interference
EN	European Norm
ERTMS	European Railway Train Management System
ESAC	Engineering Safety and Assurance Case
ESAP	Engineering Safety and Assurance Process
ESM	Engineering safety Management
ETCS	European Train Control System
EU	European Union
FET	Fault-Event Tree

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

Acronym	Definition
CCTV	Television system
PAD	Parametric Data Set
PD	Position Detector
PDD	Project Definition Document
PFI	Private Finance Initiative
PHA	Preliminary Hazard Identification
PKP	Polskie Koleje Panstwowe (Polish railway authorities)
PM	Protected Manual (mode of operation of the new train)
PMF	Project Management Framework
PPP	Public Private Partnership
PSR	Permanent Speed Restriction
PTI	Passenger Train Interface
QRA	Quantified Risk Assessment
RAM	Reliability, Availability and Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RBD	Reliability Block Diagram
RM	Route Manual (mode of operation of the new train)
RSF	Right Side Failure
RSSB	Railway Safety and Standards Board
SAA	Station Area Accident
SCC	Service Control Centre
SCID	System Context and Interface Diagrams
SDO	Selective Door Opening
SER	Signalling Equipment Room
SHL	System Hazard Log
SHWW	Sandbach/Wilmslow (geographical area of railway)
SIL	Safety Integrity Level
SM	Slow Manual (mode of operation of the new train)
SSC	System Safety Case
SSL	Sub-Surface Lines
SSR	Sub Surface Railway
SUP	Subsurface Lines Upgrade Programme
TEN	Train European Network
THR	Tolerable Hazard Rate
TPWS	Train Protection and Warning System
TSI	Technical Specification for Interoperability
TSR	Temporary Speed Restriction
UNISIG	(European) Union Industry OF Signalling

Acronym	Definition
VAF	Value of Avoiding a Fatality
VL	Victoria Line
VLU	Victoria Line Upgrade
VLUP	Victoria Line Upgrade Programme
VPF	Value Preventing Fatality
WCMU	West Coast Management Unit
WRI	Wheel Rail Interface
WRSL	Westinghouse Rail Systems Limited
WSF	Wrong Side Failure

Table 1-1: Acronyms and Abbreviations

CHAPTER TWO

PROBLEM DEFINITION

2.1 Chapter Introduction

This chapter presents the findings of the research against the history of the perception and understanding of uncertainty and risk, as well as the investigation of the existing theoretical and analytical framework in relation to the treatment of safety in engineering.

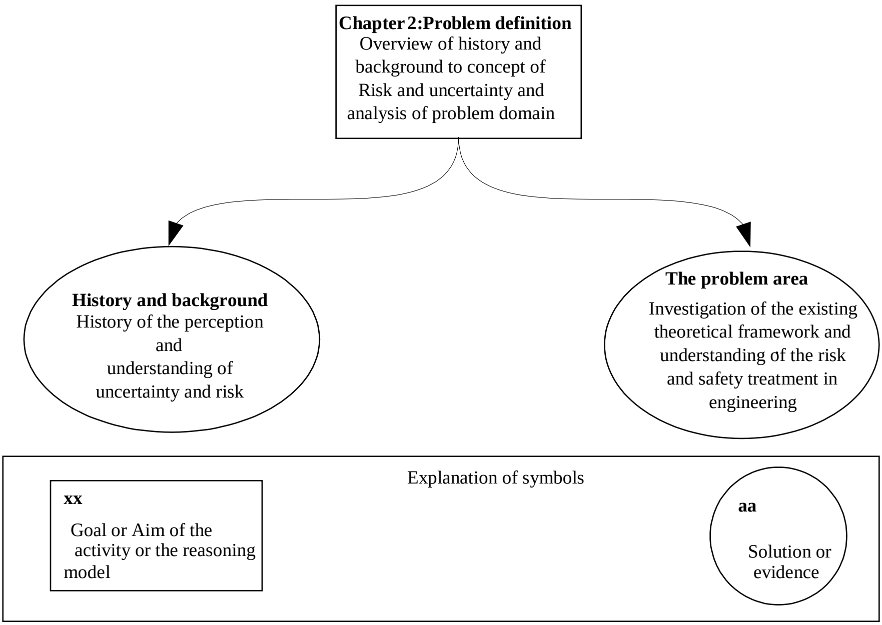

Figure 2-1: Structure of Chapter 2

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

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

This ability of our mind to perform sometimes complex statistical analysis is often sufficient. Still, situations where one could benefit from a more sophisticated treatment of issues are many.

Unfortunately, ignorance about the scientific advances in this field, as well as far too much confidence in intuition, prevents one from gaining benefits by using powerful and, more often than not, simple sets of tools provided by probability, statistics and the sciences of dynamical systems and stochastic processes.

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

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

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

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

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

Depending on different religions and cultures, for people of ancient times, the future was either a matter of luck or the result of the closeness