RAMS MANAGEMENT OF RAILWAY SYSTEMS

INTEGRATION OF RAMS MANAGEMENT INTO RAILWAY SYSTEMS ENGINEERING

By

Mun Gyu Park

A thesis submitted to the
University of Birmingham
for the Degree of
DOCTOR OF PHILOSOPHY

School of Civil Engineering
College of Engineering and Physical Sciences
University of Birmingham
August 2013

DECLARATION

I declare that this thesis is my own account for the integration of RAMS management into railway systems engineering and it contains the main research results achieved, which has not previously been submitted or published for a degree at any tertiary education institute.

………………

Mun Gyu Park

ABSTRACT

Railway RAMS is an engineering discipline that integrates reliability, availability, maintainability and safety characteristics appropriate to the operational objectives of a railway system into the inherent product design property through railway systems engineering. In the recent years it has become a rapidly growing engineering discipline because it can achieve a defined railway traffic service timely, safely and cost effectively. It also has a great potential to improve the competitiveness of railway against other transports, especially road transport. Therefore, RAMS management becomes a significant issue in today's global railway projects and it is gradually being expanded so far as to domestic railway projects.

Railway organisations have addressed the study for a long period to integrate RAMS managment into railway systems engineering, but yet only a few have implemented the RAMS management with the railway systems engineering. The major challenge of this study is to establish a systematic approach of RAMS management for railway systems engineering from the system concept phase through the establishment of the engineering concepts, methods, techniques and tools. Therefore, this research focuses on developing a systematic method for the integration of RAMS management into railway systems engineering.

This research is conducted for three research subjects and a case study. Firstly, this research provides a railway RAMS management systems so that railway organisations can decide a strategic policy, control functions and coordinate activities related to RAMS management in a systematic aspect. This research thus establishes two processes, RAMS management and railway systems engineering, to provide a fundamental basis of the RAMS management systems. Secondly, this research provides railway risk assessment methods, based on the combination of FMEA and FTA, to assess all of the potential hazards that threaten the railway’s operational objectives and control them within the possible acceptable criteria. Thirdly, this research provides the method that develops RAMS performance specifications appropriate to the RAMS requirements and operational contexts to develop RAMS design and its acceptance criteria for the detailed system design and/or contract. Finally, this research presents a case study for the risk assessment of rail vehicle pneumatic braking unit, using the field data collected from the railway industry to demonstrate the proposed assessment method of railway risks and investigate the RAMS performance of the pneumatic braking unit and their major failure causes.

This research provides a comprehensive approach for the application of RAMS management to railway systems engineering. The proposed models, methods and techniques for RAMS management will support the railway organisations that need the optimal solutions for the current issues and challenges related to RAMS management.

ACKNOWLEDGEMENTS

This thesis is submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy at University of Birmingham. During the implementation of this research project, I have benefited from communications with many colleagues, who have provided the assistance for the development of this thesis.

First of all, I would like to express sincere thanks to my supervisor, Dr Min An, for his generous help, encouragement and advice throughout the research period. I will always remember his kindness, patience and assistance not only on the technical matters, but also with my life and health issues. In addition, I would like to express my deepest gratitude for providing me an opportunity for this research.

I am particularly grateful to Prof M. Song of Korean Railroad College, Mr S. Choi of ROTECO, and Mr S. Kim of SMRTC, for their advice and support, and all professional members of the Korean Rolling Stock for their valuable advice, support, suggestions and comments. In particular, I would like to thank Mr C. Yoon, Mr J. Kim and Mr J. Park, SMRTC, for providing data and sharing knowledge on railways.

I would like to express the warmest thank to my parents and brothers for providing the research opportunity to me and supporting me financially and emotionally. Research requires a lot of time, which is usually taken with the passionate support and the deep concern of my family. Therefore, I would like to thank my wife, Hyun-Mi, and my three lovely daughters, Ji-Eun, Jae-Eun and Jung-Eun, for their continued encouragement throughout the research period as well as their practical support in English. Without their unending support and constant encouragement, this work would never have been completed.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ADV	Automatic Drain Valve
AGREE	Advisory Group on Reliability of Electronic Equipment
ALARP	As Low As Reasonably Practicable
AMSAA	Army Material Systems Analysis Activity
ARINIC	Aeronautical Radio, Incorporated
BCU	Braking Control Unit
BS	British
CA	Criticality Analysis
CENELEC	European Commit for Electrical Standardisation
ECU	Electrical Control Unit
EIA	Energy Information Administration
EN	European
EPV	Electric Pneumatic Change Relay Valve
ETA	Event Tree Analysis
FA	Functional Analysis
FAST	Functional Analysis System Technique
FCA	Failure Consequence Analysis
FDF	Fuzzy Decision Function
FFP	Failure Frequency Parameter
FI	Fuzzy Inference
FLA	Fuzzy Logic Analysis
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode, Effect and Criticality Analysis
FS	Fuzzy Set
FSP	Failure Severity Parameter
FTA	Fault Tree Analysis
HAZID	Hazard Identification
HAZOP	Hazard and Operability Analysis
HDBK	Hand Book

IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
MCS	Minimal Cut Set
MIL	Military
MR	Maintenance Rate
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MUT	Mean Up Time
NHPP	Non-Homogeneous Poisson Process
OT	Operating Time
PBS	Pneumatic Braking Unit
PDCA	Plan, Do, Check & Act
PHA	Preliminary Hazard Analysis
PRA	Probabilistic Risk Analysis
RAM	Reliability, Availability and Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RBD	Reliability Block Diagram
RCM	Reliability Centre Maintenance
RGA	Reliability Growth Assessment
RL	Risk Level
RPN	Risk Priority Number
RRR	Rapid Risk Ranking
SADT	Structure Analysis and Design Technique
SAE	Society of Automotive Engineers
ST	Standby Time
STD	Standard
TALDT	Total Administrative Logistic Delay Time
TCM	Total Corrective Maintenance Time
TDT	Total Down Time
TMT	Total Maintenance Time

TPM	Total Preventive Maintenance Time
$TSTE$	Truncated Sequential Test
TUT	Total Up Time
US	United States

LIST OF NOTATIONS

T	Top Event
M	Minimal Cut Set
X_n	Basic Events
$P(T)$	Probability of Top Event
t	Time (interval)
$R(t)$	Reliability
$F(t)$	Failure Rate
A_o	Operational Availability
A_i	Inherent Availability
A_a	Achieved Availability
λ	Failure Rate
A_s	Service Availability
$P_r(r)$	Failure Frequency Probability
$P_1(r)$	Failure Frequency Probability of Lower Limit MTBF
$P_0(r)$	Failure Frequency Probability of Upper Limit MTBF
r	Failure Frequency
r_o	Truncated Test Failure Number
m	Unknown MTBF
m_o	Upper Limit MTBF
m_1	Lower Limit MTBF
α	Producer Risk
β	Customer Risk
D	Discrimination Ratio
T_o	Truncated Test Time
$T_{a.min}$	Minimum Test Time

Chapter 1

INTRODUCTION

1.1 Motivation of the Research

The present form of railways, in which rolling stock is guided by the metal contact between rail track and rolling stock wheels, made an appearance in the mining industry of the United Kingdom in the early 19th century. The high technical effectiveness of rolling stock's metal contact and its exclusive running on the rail track without any interruption provided many excellent competitive advantages, compared to other forms of transportation, for example, high speed operating, long distance driving, large capacity transport, low energy consumption, environmentally friendly impact, high safety, consistent punctuality etc. Thus, the advantages of railways have provided a great opportunity for the massive growth of railway transport all over the world (Profillidis, 2007).

On the other hand, with the continued development and enhancement of the road and aviation transport industries, such as buses, trucks, private cars and airplanes, the role of railways in the transport sector has rapidly declined and eventually railway organisations, in most countries, have been nationalised to keep their rail traffic service. This is due to the importance of the role of railway in the population movement and national economy. As a result, the nationalisation of railways brought many negative effects to the railway organisations, for example, inflexibility, non-cost effectiveness, low quality of rail service, lack of punctuality at operation etc. However, railway organisations have brought about the turning point which has improved the above railway problems as well as cost effectiveness, availability and safety expectation in the technical and management aspects (Profilliids, 2007).

Railway organisations have been in a long search for their competitive advantages as a unique transport. For this purpose, railway organisations are now entering a specific restructuring period for the innovative improvement of their management and the application of the advanced technologies, which focus on availability, safety and cost effectiveness, for instance, the gradual liberalisation and deregulation of transport activity, the vertical separation of infrastructures from operation, the introduction of intra-mode competition, and inter-operability of railway operations for horizontal railway integration (Cantos & Compos, 2005; Profilliids, 2007).

Safety, availability and cost effectiveness are the most important issues in today’s global railway business and domestic railway environment as well. Therefore, the requirement for the railway system, capable of achieving high safety, availability and cost effectiveness, should be continuously increased in the railway industry. Accordingly, railway organisations have considered the introduction of specific engineerings in their railway design and development project. For example, RAMS management with systems engineering have been attempted by many railway organisations to establish the engineering concepts of safety, availability and cost effectivenss from the early railway project stage (BS EN 50126-1, 1999).

RAMS management is an engineering discipline that integrates reliability, availability, maintainability and safety characteristics into an inherent system design property through systems engineering process to achieve a defined railway traffic service successfully (BS EN 60300-1, 2004). In recent years, it has become a rapidly growing engineering discipline because of being able to provide a defined rail traffic service timely, safely and cost effectively. It also has a great potential to improve the competitiveness of railway against other transport sectors. Therefore, RAMS management has risen as a significant issue in today’s global railway businesses and it is being gradually expanded into the domestic railway businesses (BS EN 50126-3, 2006).

The European railway organisations have already applied RAMS management to their railway systems engineering projects. However, most railway organisations are still at the infant stage in implementing the RAMS management and systems engineering. Although the systems engineering in the railway design and development project has been applied, RAMS managment has not yet been performed in the systems engineering as a major part of the engineering management. Consequently, RAMS management has not been fully implemented. Therefore, it becomes a very significant challenge to integrate RAMS management into railway systems engineering process (Ju et al., 2011).

Many efforts have been made over a long period of time to integrate RAMS management into railway systems engineering process; however, only a few organisations have performed it due to the lack of the systematic approach of RAMS management for railway systems engineering, based on the established engineering concepts, methods, techniques and tools (Valkokari et al., 2012). Therefore, this research project focuses on the development of the systematic approach for the effective integration of RAMS management into railway systems engineering process, based on a survey of current problems and challenges of railway organisations related to RAMS management.

1.2 Railway RAMS Management

The technical performance of railway systems, such as high speed running, long distance driving and high capacity transport in the railway traffic service, has been dramatically improved over the recent years. However, the operational performance, such as availability, safety and cost effectiveness, have not made significant progress. Such low operational performance has had an adverse influence on the quality of railway traffic service and the improvement of the railway's competitiveness in the transport sector, for example, the frequent delay of the railway service, the increase of total ownership cost, and even the continuous increase of the potential damage for humans and environments caused rail accidents. Thus, RAMS management becomes a significant decision making factor in today's global and domestic railway business. Many railway organisations have continuously addressed the introduction of RAMS management in an effort to improve the operational effectiveness (Profillids, 2007).

RAMS management optimally allocates the limited resources to the system products through the railway systems engineering process. Accordingly, much attention has been paid to RAMS management from the early system concept phase. RAMS management is a professional engineering discipline which was originated from reliability and safety engineering for the improvement of the operational objectives of system. It was first introduced as part of an overall engineering discipline by the aerospace industry to evaluate the reliability and safety of aircrafts. It has continuously been further developed and applied to many industrial areas, especially in the mission and safety critical industries (An, 2005).

Since the 1980s, RAMS management has been widely adopted with the rapid development of systems engineering to effectively define, identify, assess and control all potential threats affecting the achievement of the operational objectives of a system. RAMS management in the mission and safety critical systems, such as aircraft and railway, has been developed as a distinct engineering discipline, which has established the engineering concepts, methods, techniques, measurable parameters and mathematical tools (Villemeur, 1992; An, 2005).

In particular, railway organisations have applied RAMS management in the long term operational aspects to achieve the defined operational effectiveness. The RAMS management has generally applied three aspects in the railway systems engineering project: (1) the definition of RAMS characteristics, such as reliability, availability, maintainability and safety, proper to RAMS requirements and operational contexts, (2) the assessment and control of the potential threats, such as faults, failures and errors, that affect the quality of rail traffic service and (3) the provision of the controlling means, such as failure prevention, fault tolerance, fault removal and fault prediction (BS EN 50126-1, 1999; Ucla et al., 2001; Lundteigen et al., 2009).

The railway risks that affect the quality of the defined rail service adversely and directly are the major focus of RAMS management in the railway systems engineering. Many inherent risks identified within railway systems, and the challenges which have been posed from railway systems design and development projects should require their continuous improvement from the early concept design stage throughout the whole system life cycle. The railway risks have a great potential to cause injury and/or loss of life of staffs and passengers, environmental degradation, damage to railway property or freight, and adverse economic impacts. Therefore, railway risks may require a systematic approach as a major mangement part of the railway systems engineering (BS EN 50126-2, 2007; BS ISO/IEC 26702, 2007).

The risk management approach of railway systems engineering in this context may be considered in the aspect of RAMS management in order to reduce or eliminate railway risks effectively and continuousally. The RAMS management should be established from the early system concept design stage and it should be required in the technical aspect to define, assess and control all possible risks. It is also necessary to be implemented in the management perspective to enable the quick responses to the changes of the engineering, technology, policy and/or objectives and to improve the RAMS performance continuously (BS EN 60300-1, 2003).

The risk based RAMS management for the railway systems engineering could be achieved through the development of an appropriate management systems. The RAMS management systems requires the optimal process and various techniques to ensure that RAMS organisations decide on a strategic management policy and objectives, control the management functions, and coordinate the manangement activities. The systems approach to RAMS management is necessary to achieve the following objectives: (1) to integrate RAMS management effectively into the railway systems engineering process, (2) to perform RAMS management consistently as an integrated part of the overall railway systems management, (3) to achieve RAMS requirements and operational objectives successfully and (4) to improve the system product and organisation’s performance continuously. Figure 1.1 describes the basic concept of RAMS management for railway systems engineering that will be addressed through this research project (BS ISO 9000, 2005; BS EN 60300-1, 2003).

The RAMS management systems shall be rquired to establish the policy, functions and activities of the RAMS management and to implement them through RAMS management process. It is also required to measure, assess and improve the effectiveness of RAMS management systems and the achievement of RAMS requirements as shown in Figure 1.1. The RAMS management systems shall be always performed in the system engineering project to meet the needs of customers and their expectations effectively and even to exceed them.

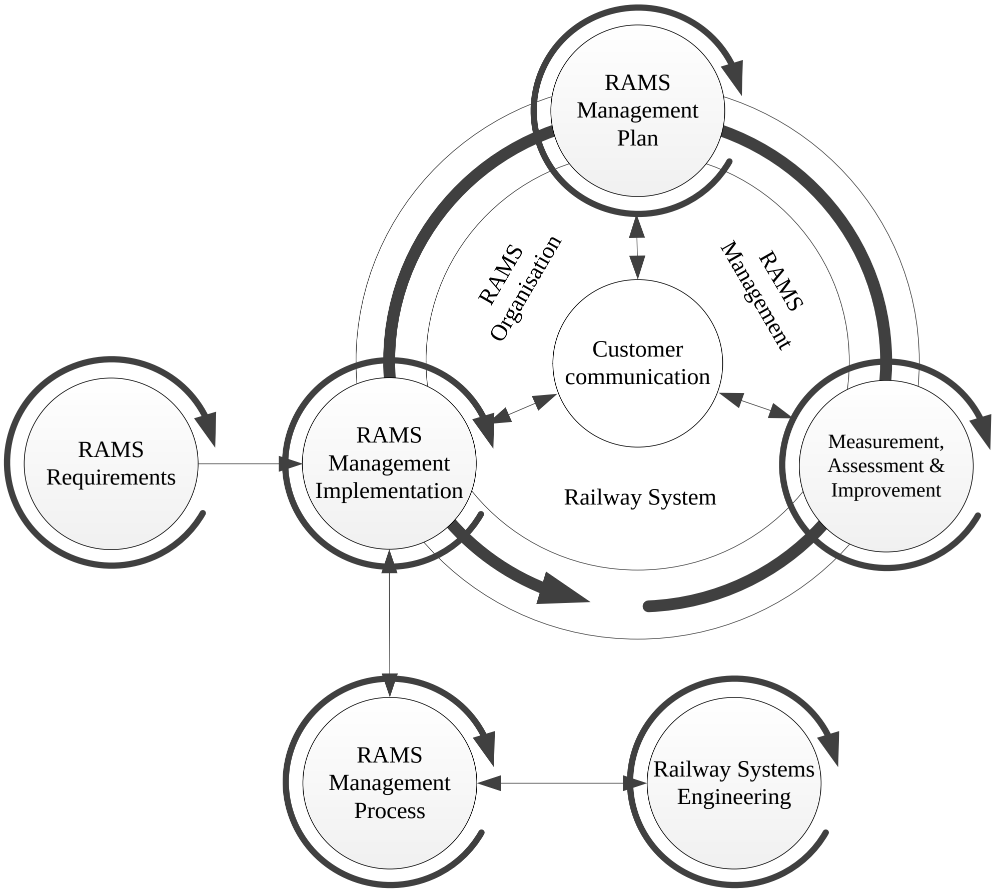


Figure 1.1 Concept of Railway RAMS Management

1.3 Major Approaches for the Research Subjects

In the previous section, the necessity of introducing RAMS management into railway systems engineering project and systems approach to RAMS management are discussed in detail, which clarify the need of further research associated with RAMS management based on the principle of systems engineering. As stated in Section 1.1, this research focuses on the effective integration of RAMS management into railway systems engineering process. For this purpose, this research pays great attention to the application of the following three principles in the study of RAMS management: (1) systems based RAMS management, (2) risk based RAMS management and (3) life cycle based RAMS management.

1.3.1 Systems Based RAMS Management

Systems approach to RAMS management is the study for the policy, functions and activities of RAMS management coherent to the overall systems engineering project; it allows allocating the management structure and environment of the RAMS organisation. The systems approach is thus becoming a key factor in the railway system management due to the rapidly growing complexity of railway system. It implies that RAMS organisations provide more adequate decision making and information flow. To accomplish such expectation, RAMS organisations should have an overall management system, which shall become a process to solve the management issues effectively. However, many RAMS organisations are not equipped with the management structure and environment as a system and they have implemented RAMS management without any established process. Therefore, this research addresses an attempt to apply the systems approach for the policy, functions and activities of RAMS management (Jenkins et al., 1968; BS EN 50126-1, 1999; BS EN 60300-1, 2003; BS ISO 9000, 2005).

1.3.2 Risk Based RAMS Management

Railway systems are always exposed to many potential threats affecting the successful achievement of the defined rail traffic service. Many inherent risks identified within the railway system require the continuous improvement from the early concept design stage due to a great potential to lead to injury and/or loss of personnel, environmental degradation, damage to railway’s property or freight, and adverse impacts to revenue. Thus, the railway risks need to be defined, identified, assessed and controlled in the systems engineering design process. However, railway organisations have not focused on the risk management in their railway systems engineering and RAMS management has not been conducted in the risk management aspect. Therefore, this research implements the study of RAMS management focused on the management of the railway risks (BS EN 50126-1, 1999; Nichollis, 2005; Lundteigen et al., 2009).

1.3.3 Life-cycle Based RAMS Management

A system life cycle consists of sequential stages, which cover the whole life of a system and provide a framework that plans, assesses, controls, monitors and reviews RAMS management functions and activities for engineering a system. Thus, the life cycle management provides a conceptual basis to ensure the high feasibility of the system in the operation and maintenance phase. The life cycle management is more commonplace in many different industry sectors. In railways, customers are highly interested in the life cycle management and the requirements have been increased continuously. However, railway organisations have not applied the concept of the system life cycle to RAMS management. Therefore, this research focuses on the establishment of life cycle functions and activities in the RAMS management (BS EN 50126-1, 1999; Hankins, 2007).

In this research, the above three approaches for RAMS management will be studied and further developments will be made, which will provide a fundamental basis to find and resolve the major RAMS management issues through systems engineering.

1.4 Research Outcomes

This research focuses on three subjects and a case study as well as theoretical background for establishing railway RAMS management. The major research outcomes are as followings:

- Literature survey of the current best practices for systems engineering, systems RAMS management, systems risk assessment and RAMS management techniques.

- Railway RAMS management systems framework, including railway systems engineering and RAMS management process for integrating the issue of RAMS management into railway systems engineering.
- Railway RAMS risk assessment framework, providing a cornerstone where all potential risks related to railway system can be defined, identified, analysed and evaluated effectively and efficiently.
- Railway RAMS performance specification framework to facilitate the detailed design and contract to both customers and suppliers.
- A case study that demonstrates the risk assessment model and identifies the risk level of railway vehicle pneumatic braking unit.

In addition, three research papers have been presented in the international railway conferences and a journal paper is being prepared. They are:

1. M. Park, M. An, and Felix Schemid (2009), *A Study on decision of rail vehicle maintenance policy:* Proceeding of the 10th International Railway Engineering Conference, Theme 1: Railway Vehicle Technology & Maintenance (RVT), London.

2. M. Park and M. An (2010), *Development of a framework for engineering RAMS into rolling stock through life cycle in the operator perspective*. Proceeding of the 10th Korean Railway Conference, Seoul, pp. 2179 – 2194.

3. M. Park and M. An (2011), *A methodology for rolling stock RAM target setting demonstration*. Proceeding of the 11th International Railway Conference, London, CD: ISBN 0-947644-69-5.

(Please see Appendix)

4. M. Park and M. An (2013), A railway vehicle RAMS risk management - The FMEA-FTA approach and RAMS Management process approaches: a case study.

1.5 Outlines of Research Thesis

This thesis comprises eight chapters to discuss a methodology for the introduction of RAMS management into railway systems engineering. The main contributions of this research are included in Chapters 4 to 6. The main formulation of this research are discussed in Chapters 2 and 3. Chapter 7 provides a case study and the main achievements of this research are concluded in Chapter 8. Brief summaries of each chapter are given below:

Chapter 1 presents an overview of this research as an introduction. This chapter firstly discusses the background of this research project. This chapter also presents railway RAMS management for the successful achievement of the defined rail service objectives and the systems approach of RAMS management to railway systems engineering. Three approach principles are defined as the basis of this research project. The major issues and challenges of RAMS management are discussed as well. Finally, the subsequent chapters are summarised briefly.

Chapter 2: This chapter presents the research methodology adopted to conduct this research successfully. This chapter begins with the identification of the current problems and challenges related to RAMS management; thus, the research questions are developed, and the research purpose and objectives are established. The research methods adopted to find the solutions related to the major research issues are described in detail. The research process and plan are finally discussed in this chapter.

Chapter 3: This chapter presents an extensive literature review to provide a conceptual review of systems engineering and to investigate the engineering concepts, methods and techniques related to RAMS management. This chapter firstly reviews the engineering and management concepts of successfully realising a system. The concept of systems RAMS management in three aspects is discussed. The definition of railway risks and their assessment methods are presented, and the important techniques for RAMS management are briefly investigated for their substantial objectives, advantages and disadvantages.

Chapter 4: In this chapter, the concepts of systems approach to RAMS management for railway systems engineering are enumerated and a management systems is provided to establish the foundations for organising the management structure and environment of RAMS organisation. This chapter describes the two management processes: systems engineering and risk based RAMS management process. The systems engineering process is to provide a basic foundation of the functions and activities related to RAMS management, and the risk based RAMS management process is to provide the appropriate control of all possible railway risks.

Chapter 5: This chapter presents the development of railway risk assessment method based on the integrated FMEA and FTA techniques and its application process. The principles of FMEA and FTA approaches for the definition of railway risk are described in detail and two FMEA-FTA combination models are developed to apply them to the system engineering design phase. The FMEA-FTA based risk assessment process is demonstrated with phased descriptions providing several examples to explain the FTA mathematically.

Chapter 6: This chapter presents a precise performance specification method for resolving the RAMS design and acceptance issues to be solved by the system design. This chapter discusses a framework for the performance specifications of railway RAMS requirements and operational contexts, including the definition of railway RAMS elements and the principles and process of RAMS performance specifications. The specification process that can specify the RAMS performance for operational requirements at different system design phases are also discussed in this chapter.

Chapter 7: This chapter provides a case study for the risk assessment of rail vehicle pneumatic braking unit in order to illustrate the practical application of the proposed FMEA-FTA based railway risk assessment method. This includes identifying the major failure causes that lead to a full service braking error in the operational situations, and evaluating the risk level and operational reliability performance. This chapter begins with the detailed description on the pneumatic braking unit and then describes how FMEA and FTA analysis, using information and data collected from the railway field, is used in the risk assessment process.

Chapter 8: This chapter provides the research results for how the purpose and objectives of the research are accomplished by the research methodology selected in the research project. Recommendations for implementation of further research work are finally given in this chapter.

Chapter 2

RESEARCH METHODOLOGY

2.1 Introduction

This chapter explains the research methodology adopted to conduct this research project effectively. This chapter commences with the definition of this research through the survey of the current problems and challenges related to RAMS management investigated from the railway industry. The identified problems and challenges are subsequently analysed to establish the research questions and determine the research purpose and objectives. RAMS management and systems engineering in the railway project are a relatively new engineering discipline. Accordingly, the industrial approach for their issues and challenges is greatly limited. Thus, this chapter secondly presents the several research methods adopted for identifying the issues and challenges of RAMS management and finding their solutions from railway organisations. Finally, the research process and schedule planned to achieve the research objectives are designed effectively.

The subsequent chapters will be dedicated to the study of the research subjects and a case study through the effective application of the research methodology adopted. The research methodology is applied to identify the research issues and challenges to be considered and it is conducted for the assessment[1] of the research issues to continuously improve the major issues associated with this research subject. This chapter consists of five sections to discuss the research methodology adapted. Section 2.2 defines the research subjects through the analysis of current problems and challenges related to RAMS management. Section 2.3

[1] Assessment is a process that needs the activities of definition, identification, analysis and evaluation.

presents the research methods adopted to perform the research subjects and the research process and scheduled plans are provided in Section 2.4. This chapter finally gives a brief summary in Section 2.5.

2.2 Research Definition

2.2.1 Problem and Challenge Statement

Railway design and development projects have been conducted in a complex engineering environments where many interrelated, typical engineering disciplines[2] are worked in an integrated engineering process simultaneoulsy. However, RAMS management and systems engineering among the railway engineering disciplines have been mostly tacit engineering disciplines in spite of the high requirements and expectations of the railway industry. Although RAMS management has been implemented in the railway engineering project, it was highly dependant on the individual and organisational experience, perception and know-how. The RAMS management has not implemented systematic approach to railway systems engineering. Therefore, due to such railway situations RAMS management cannot help including many challenges and problems to be improved (Carretero et al., 2003).

Several examples which was failed in the introduction of RAMS management into railway systems engineering have existed in the various lines of the railway projects. Some of the reasons why RAMS management was problematic or failed were down to technical issues in essence, but, as a matter of fact, the majority of the reasons were confirmed from the railway organisations that implement RAMS management (Carretero et al., 2003). RAMS management supports the operational decision making, such as availability, safety and cost effecctiveness, of the railway systems engineering. Accordingly, the introduction of systems

[2] Mechanical, Electrical, Electronics, Civil and Software Engineering

engineering in the railway project is essential to implement RAMS management. However, RAMS management have not been completely integrated into the railway systems engineering project or even it have not been included. Therefore, the introduction of systems engineering in a railway project is a prerequiste condition for the implementation of RAMS management (Fiet, 2010; Morfis, 2009).

Railway organisations should have formal processes for sharing and assessing information and data related to railway risks to enable the implementation of RAMS management timely and to avoid the repeated management activities. However, the information and data related to railway risks are not processed into information sources by appropriate methods and most of which are also statistically inadequate. In particular, the risk information and data related to human errors and their assessment techniques are not yet established. The data and information sources are not systematically collected in the perspective of system engineering and RAMS management (An, 2005; Valkokari et al., 2012).

RAMS management requires the knowledge of system sciences and engineering, appled in the stages of the system life cycle. It currently demands the adequate perception of risk and systems approach. Furthermore, systems thinking and life cycle management are also essential for RAMS management. However, these are not included in the RAMS mangement. Customers have had difficulty in expressing their requirements, for example, availability and safety of the system and its life cycle, based on the accurate numerical values where possible. Also, on occasions, suppliers have not provided the precise technical RAMS design criteria (Blanchard, 2012; Valkokari et al., 2012).

These challenges and problems that have affected RAMS management call for a more coherent and structured approach for the systems engineering and RAMS management.

Therefore, it is essential to develop a model for a new approach of RAMS management which satisfies the needs and expectations of the railway organisations.

2.2.2 Research Questions

Three research questions are discussed based on the challenges and problems as stated in Section 2.2.1. These questions purport to seek the theoretical backgrounds that are essential to the research subjects.

Difficulties in designing RAMS characteristics, such as reliability, availability, maintainability and safety, into the system product property, have been lessoned from other industries because there is very little literature reporting the reasons for such difficulties. Knowledge of the system sciences and engineering is a fundamental in the research project. On the basis of this reasoning, the first research question has been formulated as follow:

- How can a system be realised in the systems engineering project and how can RAMS characteristics be designed as a design property of the system products?

As a complex system which has applied many advanced technologies, railway systems include many hazards that may cause various failures and accidents. Accordingly, the appropriate risk assessment of railway hazards is a key factor when designing a safe, dependable and cost effective railway system. Another issue of interest in the research project is how to minimise or eliminate the possible threats within the acceptable range of the project, which affect the operational objectives. The following reasoning, the second research question has been formulated as follow:

- How can all potential hazard factors that threaten the operational objectives of a system be defined, identified, assessed and controlled?

Systems RAMS is an inherent product design property of a system. The performance of RAMS characteristics is achieved through the system engineering design process. Thus, it is very important to determine the RAMS design and acceptance criteria in the railway engineering project. The final issue of interest in this research is to transform RAMS requirements and operational contexts into technical RAMS design and acceptance criteria for implementation of the system detailed design and/or project contract. On this basis, the following research question has been formulated:

- How can the technical RAMS design and acceptance criteria be quantitatively specified for implementation of the system product design and project contract?

2.2.3 Research Purpose and Objectives

2.2.3.1 Research Purpose

The purpose of this research is to develop a systematic approach for integrating RAMS management into a railway systems engineering project to successfully achieve the operational objectives, such as availability, safety and cost effectiveness. The methodology developed in this study will help railway organisations in establishing their policy, objectives, functions and activities for the RAMS management in the railway systems engineering projects.

2.2.3.2 Research Objectives

The objectives of this research are to ensure the successful implementation of the above research purpose. They are:

- To establish the concepts of systems engineering and RAMS management and investigate the processes, methods and techniques to effectively support RAMS management as used in practice and literature;

- To develop a systematic approach of RAMS management for railway systems engineering;
- To provide the methods that define and assess all potential hazards that threaten the operational objectives of railway systems;
- To provide the methods that quantitstively specify RAMS requirements and operational contexts into technical RAMS design and acceptance criteria;
- To conduct a case study to demonstrate the proposed risk assessment method, and;
- To provide recommendations for further implementation of RAMS management in the railway engineering project.

2.3 Research Methodology

2.3.1 Literature Review

This research establishes a broad research foundation through the investigation, understanding and analysis of various literatures. The literature review should be implemented throughout the whole research period to obtain the consolidatory basis of the research topic and to continuously improve and update the quality of the research results achieved. Therefore, the literature survey is performed in the two perspectives: (1) preliminary literature review and (2) detailed literature review.

The preliminary review has already been conducted from the early phase of this research and it aims for: (1) the establishment of the research topic, (2) the identification of the challenges and problems associated with the research topic, (3) the determination of the purpose and objectives of the research, (4) the establishment of the theoretical background, methods and techniques associated with the research subjects, (5) the development of the conceptual research models, (6) the acquisition of the research information and data needed and (7) the identification of the gaps between the best practices recommended from various industrial areas and the current capacity of the industrial fields.

The detailed literature review is carried out throughout the whole research period in order to sustain the followings: (1) the continuous improvement and upgrading of the developed conceptual research models, (2) the establishment of a deeper and wider theoretical background for the developed research models, (3) the prevention of the omission of important information related to the research subjects and (4) the continuous collection of advanced knowledge and information.

The literature review have been performed through major international engineering standards, text books, journals and conference articles. The generic models, methods and techniques associated with the research subjects are explored by well-known text books and international engineering standards. The text books provide the detailed descriptions and guidance for the general science and engineering related to each system life cycle phase. The international engineering standards provide the international engineering trends, the defined terminologies and the general guidance for the application of specific engineering activities associated with each system life cycle phase. On the other hand, the articles and journals provide some specific methods and techniques which can be used at the important decision-making points of the specific engineering (Valkokari et al., 2012).

2.3.2 Use of Interview Survey

This research applies an individual interview method to identify the current issues and challenges related to the research subjects and to evaluate the research models developed through the research. Interviewing is one of the common research methods; it can find research challenges and issues, collect the information and data related to the research topics, and lead to the solution of the research challenges and issues. Furthermore, the interview is a flexible method which can extract important ideas and useful opinions from interviewees (Bryman et al., 2007).

Most commonly, an interview is conducted on an individual basis, but group interviews, mailed questionnaire or telephone survey may also be useful methods. They will be helpful to obtain the practical challenges, problems and detailed opinions related to the research study, and improve the intended research strategies by conducting interviews to collect information from different organisations (Kendall et al., 1992; Bryman et al., 2007).

The research considers individual interview from railway experts, for example: researchers, consultants, operators and maintainers of several different railway organisations.

2.3.3 Case Study

This research conducts a case study to identify the current issues of railway systems and demonstrate the developed research models. The case study is a very useful method to understand the complex issues and challenges related to the research topic effectively. It can also expand the range of experiential know-how, background and knowledge that have been reported and recognised from the past data. The case study emphasizes the comprehensive contextual analysis of limited events, conditions and their relationships. Therefore, various case studies have been used across a variety of engineering disciplines (Ahamad, 2011).

This research implements a case study to demonstrate railway risk assessment method and investigate operational RAMS performance and major failure causes.

2.4 Research Design

This research project is step by step implemented according to the planned strategy and procedures as shown in Figures 2.1 and 2.2.

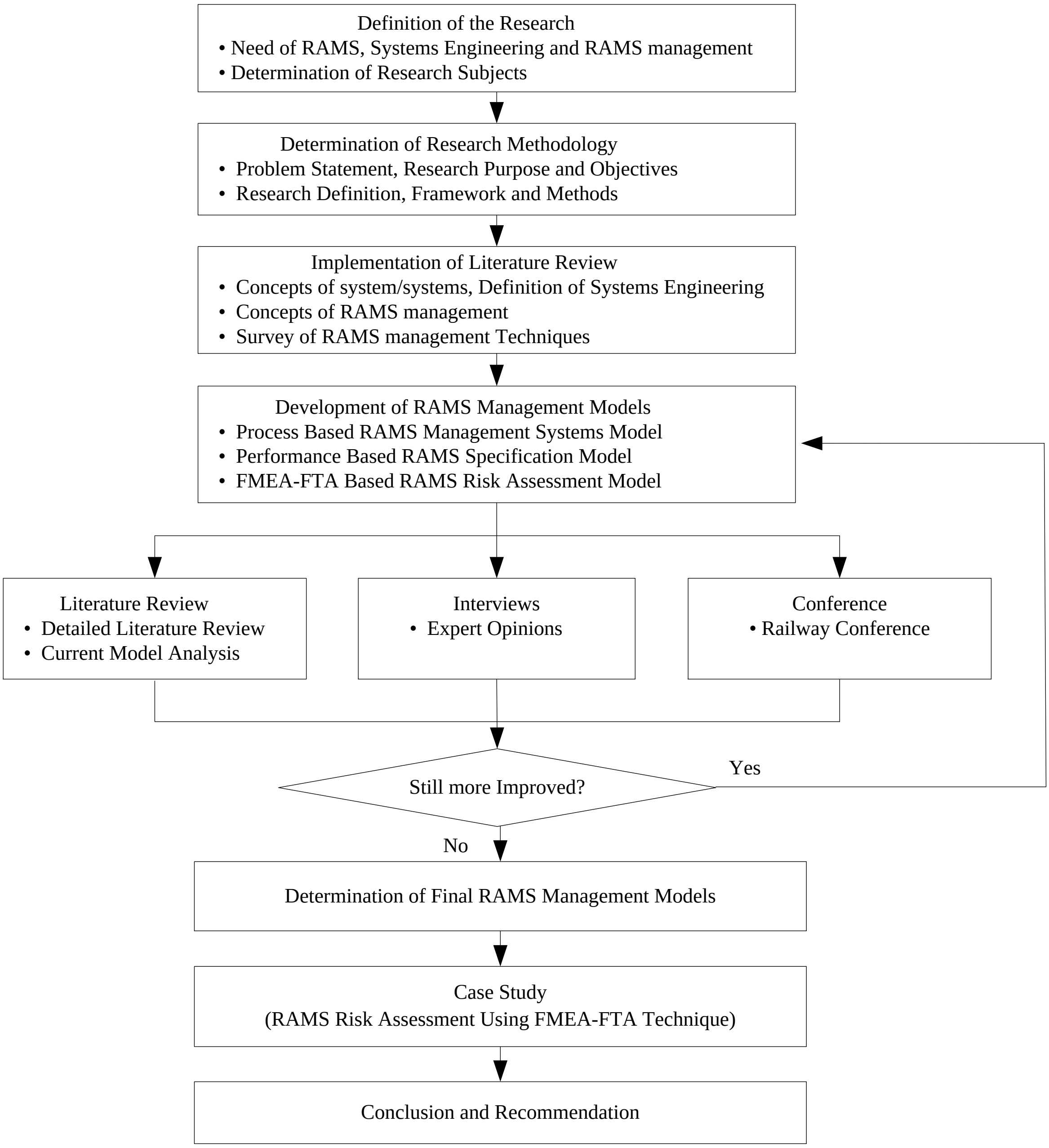
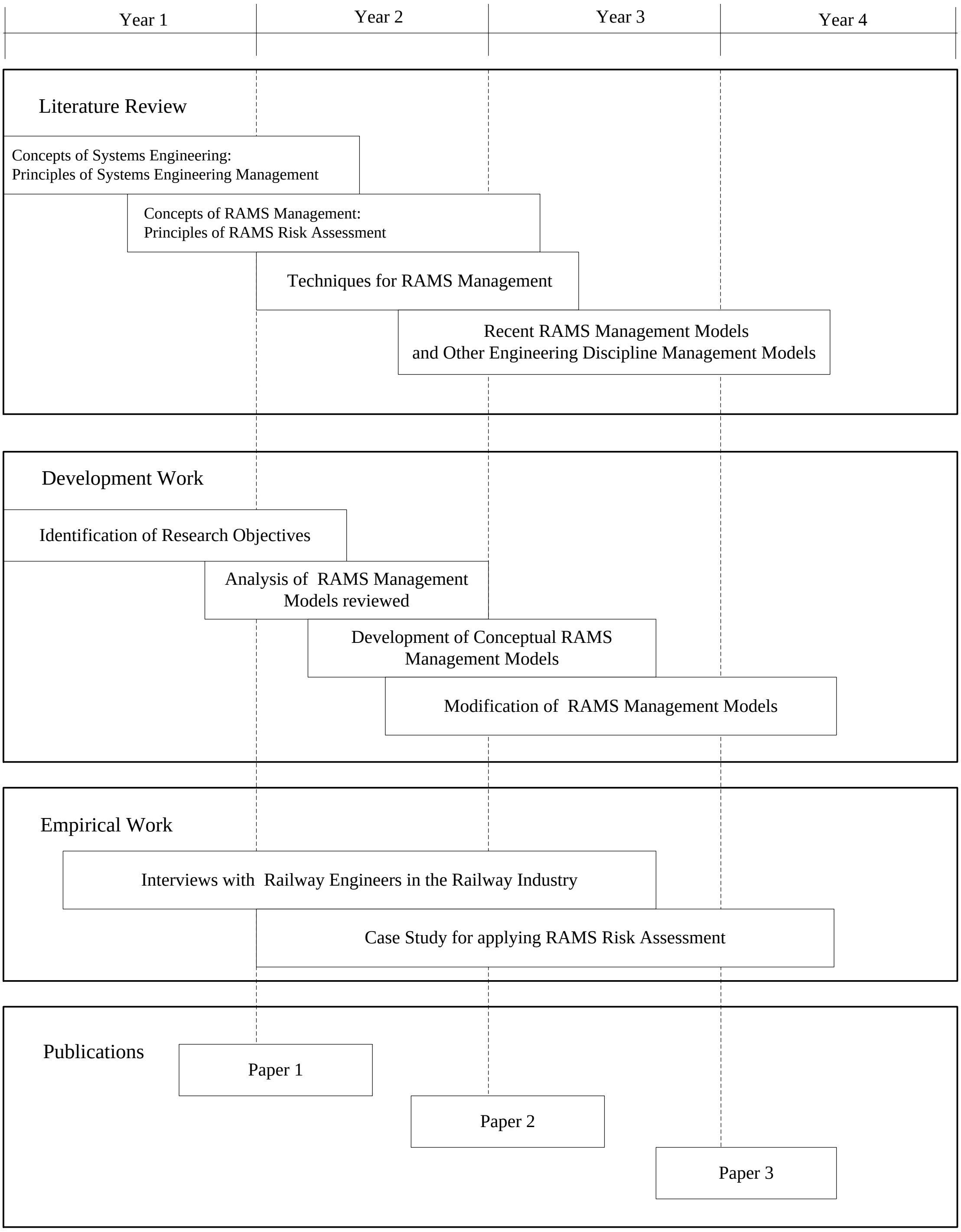

Definition of the Research
• Need of RAMS, Systems Engineering and RAMS management
• Determination of Research Subjects
Determination of Research Methodology
• Problem Statement, Research Purpose and Objectives
• Research Definition, Framework and Methods
Implementation of Literature Review
• Concepts of system/systems, Definition of Systems Engineering
• Concepts of RAMS management
• Survey of RAMS management Techniques
Development of RAMS Management Models
• Process Based RAMS Management Systems Model
• Performance Based RAMS Specification Model
• FMEA-FTA Based RAMS Risk Assessment Model
Literature Review
• Detailed Literature Review
• Current Model Analysis
Interviews
• Expert Opinions
Conference
• Railway Conference
Still more Improved?
Yes
No
Determination of Final RAMS Management Models
Case Study
(RAMS Risk Assessment Using FMEA-FTA Technique)
Conclusion and Recommendation

Figure 2.1 Research Process



Year 1
Year 2
Year 3
Year 4
Literature Review
Concepts of Systems Engineering:
Principles of Systems Engineering Management
Concepts of RAMS Management:
Principles of RAMS Risk Assessment
Techniques for RAMS Management
Recent RAMS Management Models
and Other Engineering Discipline Management Models
Development Work
Identification of Research Objectives
Analysis of RAMS Management
Models reviewed
Development of Conceptual RAMS
Management Models
Modification of RAMS Management Models
Empirical Work
Interviews with Railway Engineers in the Railway Industry
Case Study for applying RAMS Risk Assessment
Publications
Paper 1
Paper 2
Paper 3

Figure 2.2 Research Plan

Figure 2.1 describes the research process that will be performed through the whole research period. The process consists of five phases: (1) the definition of the research, such as research subjects, research purpose and objectives and research methodology, (2) the establishment of research issues through literature review, interview, survey etc., (3) the development of conceptual research models, (4) the evaluation of research results through literature review, interview and conferences and (5) the continuous improvement of research results.

Figure 2.2 describes the plan that will implement the research project during the entire research period. This research is conducted in the four areas: literature review, model development, empirical work and publications. The literature review focuses on the establishment of theoretical fundamentals associated with the research subjects. The development work concentrates on the development and continued improvement of the research models to meet the research objectives. Finally, the empirical work focuses on the finding of the solutions and identifying the gaps related to the issues of the research subjects.

2.5 Summary

This chapter has presented the research methodology adopted to perform the research project effectively and efficiently.

Firstly, this research was defined through a survey of the current challenges and problems related to the introduction of RAMS management into railway systems engineering. In the survey, the major challenges and problems confirmed the needs of RAMS management for railway systems engineering in the management perspective. The problems and challenges are based on the development of the research questions, which are reflected in the establishment of the research purpose and objectives.

RAMS management and railway systems engineering are relatively new engineering disciplines in the railway industry. Hence the industrial and organisational approach for finding out the issues, challenges and solutions related to the research subjects are greatly limited. Therefore, the planned research methods to resolve such a problem were presented and their application method was described in detail.

Finally, this chapter has presented the research process and plan to conduct the research project step by step. This research is performed over a long period of time. Therefore, the research process and plan will be upgraded and improved for the effective achievement of the research objectives. As mentioned above, RAMS management in the railway industry is a relatively new engineering discipline and the industrial approach of the RAMS management may be greatly limited. Therefore, it is anticipated that the research methodology will be modified and updated continuously.

Chapter 3

LITERATURE REVIEW

3.1 Introduction

Railway RAMS is an inherent system product property that affects the overall quality of a defined rail traffic service. The RAMS performance needed for the achievement of the operational objectives of a system can be achieved through the successful integration of RAMS characteristics into the product design of the system. Accordingly, railway systems engineering, to design the optimal RAMS characteristics at the system concept design phase, is essential for the successful implementation of RAMS management. Therefore, this chapter firstly discusses the definitions of system, systems and systems engineering, and the concepts of systems engineering management to establish a fundamental engineering basis of RAMS management (Vintr et al., 2007; BS EN 60300-3-15, 2007).

Railway system is a mission and safety critical system. Therefore, to achieve the operational objectives of a railway system, all possible potential hazards that affect the railway system must be defined, identified, assessed and controlled through RAMS management from the system concept design stage throughout the system life cycle phases. The concept of risk is defined for an effective risk assessment and the resultant risk assessment is the basis of RAMS management. Thus, this chapter reviews the concepts of risk based RAMS management and also investigates the various methods and techniques to implement the RAMS management (Pasqual et al., 2003; BS EN 50126-1, 1999).

This chapter consists of five sections to provide an extensive literature review. Section 3.2 presents the concepts and principles associated with systems engineering, followed by Section

3.3, which reviews the concept and principle of systems RAMS management and risk assessment. Section 3.4 investigates the various techniques for implementation of RAMS management. Subsequently Section 3.5 finally provides a summary of this chapter.

3.2 Concept of Systems Engineering Management

Systems engineering forms a foundation for the design and development of a system. RAMS management is a branch engineering discipline of the systems engineering. Therefore, the RAMS management is implemented as an integrated part of systems engineering (BS EN 60300-3-15, 2003). This section firstly reviews the concept of systems engineering in the management aspect to establish a theoretical background of RAMS management.

3.2.1 History of Systems Engineering

The term '*system*' derives from the Greek '*sustēma*', which means '*with set up*' or '*with an organised whole*' (Blanchard, 2012). The Oxford dictionary (2012) defines the system as "*a set of things that work together as part of a mechanism; a complex whole, a set of principles or procedures when something is done; an organized scheme or method.*" The concept of the system has been applied to many engineering disciplines, related to the large, complex mission and/or safety critical systems.

The field of natural science firstly applied 'the concept of system' in the 19th century in terms of the proposal of Nicolas Leonard Sadi Carnot (1796-1832), a French physician. On the other hand, the science and engineering field started the wider application of the system concept by 'General system theory,' published by Bertalanffy in 1945. The general system theory has been applied subsequently as a principle that designs and develops a system (Elphick, 2010; Blanchard, 2012).

The Bell Company in the United States first deployed 'the principles of systems engineering' to develop 'systems operability' in the 1940s. The principle of systems engineering has been applied to many industries in an effort to improve the competitiveness and to solve the complexity and uncertainty of a system due to the introduction of advanced technology and management. Above all, the successful implementation of 'the Apollo Spaceship Project' in the 1960s provided a big opportunity for the worldwide application of the systems engineering principle. Many railway organisations have been attempted the application of the systems engineering since the 1980s, but it is still in the infant stage (Kossiakoff et al., 2011).

3.2.2 Definition of Systems Engineering

The concept '*system and systems*' are the major principles of systems engineering and RAMS in the technical and management aspect (BS EN 50126-1, 1999).

3.2.2.1 Definition of System

There are many definitions of the term 'system' in the international standards and literature, but these definitions have some differences in the expressive degrees. The following three definitions are provided to clarify the understanding of the considerable differences between them as below:

> System (BS ISO 9000, 2005) is *"a combined set in which organised system elements interact to achieve the stated objective."*
>
> System (Hasikins et al., 2007) is *"an integrated set of system elements, for example, subsystems, components or assemblies, which achieve a defined objective. These elements include products (hardware, software and firmware), processes, people, information, techniques, facilities, services and other support elements."*
>
> System (Kapurch, 2010) is *"a constructed set of many different elements to create the desired results together, which cannot be achieved by the individual elements. The*

> *system elements can include people, hardware, software, facilities, polices and documents, namely, all things that are required to obtain the desired results in the system level. The results of the system level include system qualities, properties, characteristics, functions, behaviour and performance. The value as a whole or system level, contributed by the independent elements, is primarily created by the relationship and interaction among the elements; that is, it is very important how they are interconnected."*

3.2.2.2 Definition of Systems

The term 'systems' is an enlarged concept of the above 'system' as a major approach of the management aspect; it is often called the 'system of system' or 'system of systems'. Recently, the concept of the systems has been applied as the principle of the systems engineering in the management aspect; it has been applied to the management of the large, complex systems that are made up of many independent subsystems and/or components, for instance, an aircraft system and a railway system (BS ISO/IEC 15288, 2002; Clark, 2008; Blanchard, 2012).

In general, customers have required the application of the systems concept as an 'acceptance criteria' of the system being designed and developed, while system suppliers have applied it to develop 'technical design criteria' of the system. The systems concept is defined through the investigation of the operational behaviour and interface for the successful mission criteria of a system, for example, mission profiles, performance, availability, safety, cost etc. However, the two concepts of system and systems are not any difference in the technical aspect, but the systems concept is very important in the management aspect of systems engineering (Clark, 2008). Three different definitions of the term 'systems' are provided to clearly understand:

> Systems (Despton, 2007) is *"an organized complex unity that is assembled from dispersed, highly co-operating autonomous systems – each of which is capable of operating independently."*

> Systems (Blanchard, 2012) is *"a collection of system elements that produce results unachievable by an individual system. The individual system in the systems structure is likely to be operational in its own right, as well as be contributing in the accomplishment of some higher-level mission requirement. The life cycles of the individual systems may vary somewhat as there will be additions and deletions at different times, as long as the mission requirements for any given system are met. Thus, there may be some new developments in progress at the same time as other elements are being retired for disposal."*
>
> Systems (BS ISO/IEC 15288, 2002) is *"a man-made, created and utilized to provide services in the defined environments for the benefit of users and other stakeholders. These systems may be configured with one or more of the following: hardware, software, humans, processes (e.g., review process), procedures (e.g., operator instructions), facilities and naturally occurring entities (e.g., water, organisms, minerals). In practice, they are thought of as products or services. The perception and definition of a particular system, its architecture and its system elements, depend on an observer's interests and responsibilities; one person's system of interest can be viewed as a system element in another person's system element of interest. Conversely, it can be viewed as being part of the environment of operation for another person can be viewed as being."*

Elphick (2010) classifies the hierarchy of a railway system into three levels in the systems perspective as below and BS EN 50126-1 (1999) describes the aspects of system, subsystems and components under consideration of the system level approach as shown in Figure 3.1. However, the definition of the system, subsystem and component can be changeable under different considerations as shown in Figure 3.1:

- Level 1: A subsystem, which is defined substantially within one engineering discipline, for example, a driving gear box, an air conditioning, a bogie etc.;
- Level 2: A system, which includes two or more engineering disciplines, for example, a rolling stock, an electrical power supply, a signalling etc. and;
- Level 3: Systems, which affects or is impacted by many disciplines and economics, social or environmental factors, for example, a railway system as total system.

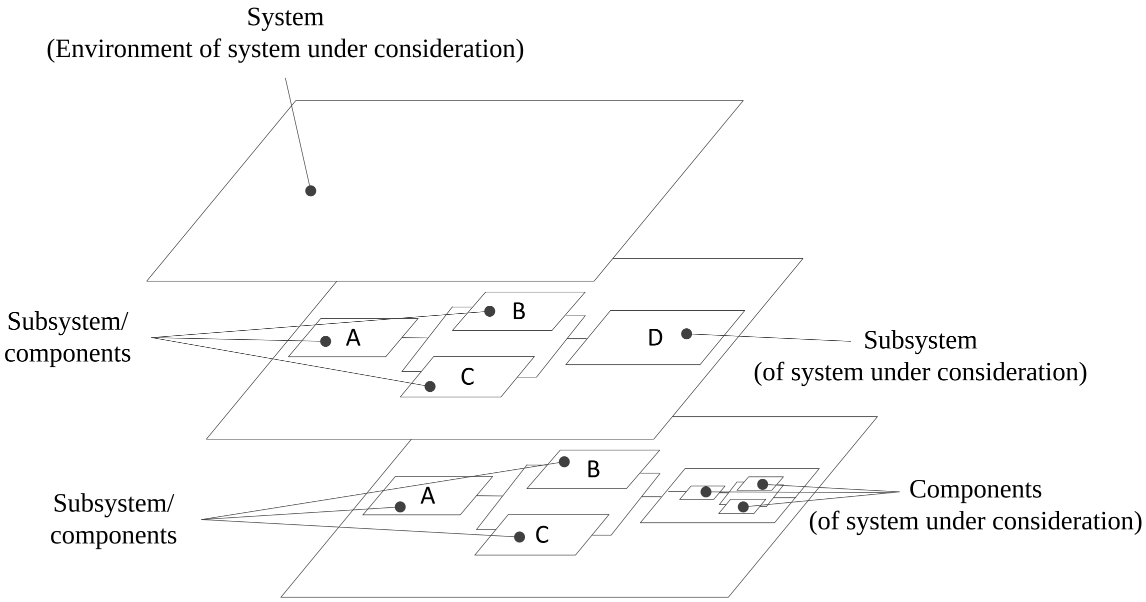

System
(Environment of system under consideration)
Subsystem/
components
A
B
C
D
Subsystem
(of system under consideration)
Subsystem/
components
A
B
C
Components
(of system under consideration)

Figure 3.1 Systems Level Approach (BS EN 50126-1, 1999)

3.2.2.3 Definition of Systems Engineering

Systems engineering is an important principle to develop the '*technical design criteria*' of a system in the system concept design phase. There are many different definitions related to the systems engineering in the international engineering standards and literature. The below three different definitions are given to help the complete understanding of the systems engineering:

> Systems Engineering (MIL-STD-499B, 1994) is *"the application of scientific and engineering efforts to:*
>
> - *Transform an operational need into a description of system performance parameters and a system configuration through the use of an iterative process of definition, synthesis, design, test and evaluation;*
> - *Integrate related technical parameters and ensure compatibility of all physical, functional and program interfaces in a manner that optimises the total system definition and design and;*
> - *Integrate reliability, maintainability, safety, survivability, human engineering and*

> *other factors into the total engineering effort to meet cost, schedule, supportability and technical performance objectives."*

Systems Engineering (Hasikins et al., 2007) is *"a discipline that concentrates on the design and application of the whole (system) as distinct from the parts. It involves looking at a problem in its entirety, taking into account all the facts and all the variables and relating the social to the technical aspect."*

Systems Engineering (BS ISO/IEC 26702, 2007) is *"an interdisciplinary approach and means to enable the realisation of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem. Systems engineering considers both the business and the technical needs of all customers with the goal of providing a quality of the product that meets the user needs."*

From the definitions of systems engineering, Kossiakoff et al. (2011) describes the difference between the systems engineering and the traditional engineering discipline (e.g., mechanical, electrical, civil engineering etc.) as below:

Systems engineering:

- is concentrated on the system as a whole;
- is focused on the customer requirements and operational contexts;
- provides the conceptual design of a system, and;
- takes the role as a bridge between traditional engineering disciplines.

Moreover, systems engineering is applied as an integral part of a project, which plans and guides the overall activities of systems engineering (Daup, 2001). Therefore, systems engineering is sometimes called systems engineering project or systems engineering management.

3.2.3 Concept of System Life Cycle

System life cycle is a very important concept in the systems engineering. A system life cycle includes the various activities that are required from the defined sequential stages from the concept to retirement as Table 3.1. Every system, regardless of its type or size, follows a defined life cycle stage. The life cycle consists of the sequential stages, as described in Table 3.1, which cover the whole life of a system and typically provide a framework that plans, assesses, controls, monitors and reviews all activities for engineering a system. Therefore, systems engineering focuses on integrating the system life cycle functions. Table 3.1 shows system life cycle stages and functions that are typically used in the systems engineering management (BS ISO/IEC 15288, 2002; Blanchard, 2012; Hasikins et al., 2007).

Table 3.1 System Life-cycle Stage (From BS ISO/IEC 15288, 2007)

Life-cycle stages	Purpose	Decision gates
Concept	• To confirm customer’s needs and expectations. • To examine concepts. • To propose viable system solutions.	Decision Options: • Conduct next stage • Continue this stage • Go to a preceding stage • Hold project activity • Terminate project
Design & Development	• To define system requirements. • To develop system solution description. • To build system products. • To verify and validate system products.	
Production	• To produce system products. • To inspect and test (to verify system products).	
Operation	• To operate system to meet customer’s needs.	
Support	• To provide the sustained capability of the system.	
Retirement	• To store, archive or dispose of the system	

3.2.4 Concept of Systems Engineering Management

Systems engineering can be conducted successfully, not only through the achievement of the technical knowledge, but also through that of the management. The establishment of an appropriate organisational environment together with the effective and efficient management structures are essential criteria for the successful implementation of systems engineering, and it assures the development of the optimal technical design and acceptance criteria which satisfy the customer’s needs and expectations of a system (Blanchard, 2012).

In general, the role of systems engineering management is for the complete integration of the following three engineering activities: (1) the control of the baselines in each design and development phase, (2) the implementation of the system engineering process and (3) the integration of the major system life cycle functions. Figure 3.2 provides the interrelationship between the systems engineering management activities, which are a basis of systems engineering management and RAMS management (Daup, 2001).

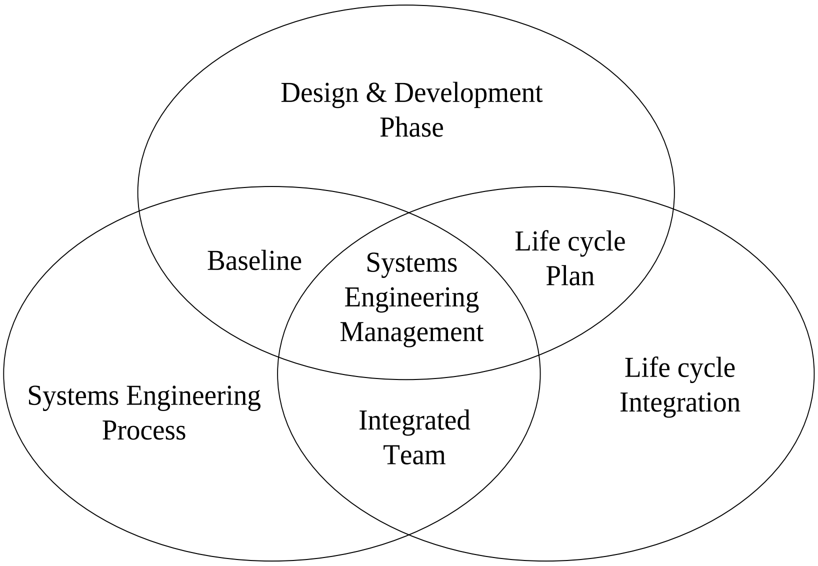

Design & Development Phase
Baseline
Systems Engineering Management
Life cycle Plan
Systems Engineering Process
Integrated Team
Life cycle Integration

Figure 3.2 Systems Engineering Management Activities (From Daup, 2001)

3.2.4.1 Control of Design and Development Phase

The control of the baseline in the design and development phase is an important role of systems engineering management. In general, a system is designed and developed progressively through several design phases; the design results are controlled in the allocated baseline phase as shown in Figure 3.3.

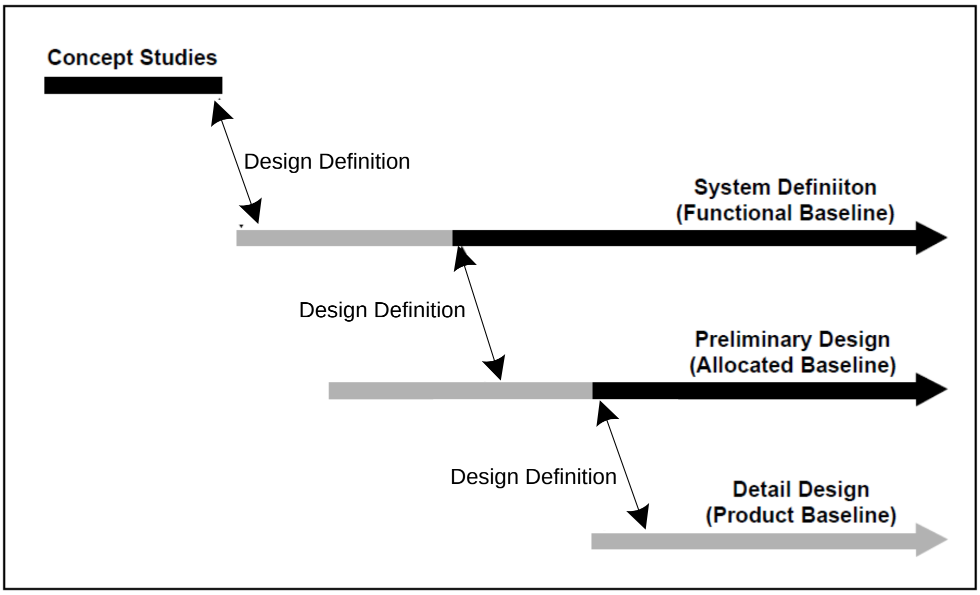


Figure 3.3 Baseline Controls of Design and Development Phase (From Daup, 2001)

The system concept phase creates the concepts of a system to design and develop; it is often called the feasibility study phase. The system definition phase provides a description for the requirements in terms of the system functions and performances and it consists of a functional baseline as shown in Figure 3.3. Finally, the preliminary and detailed design phases produce a set of the subsystem and component architectures, including the performance characteristics and design description of the system products. The preliminary design phase comprises the allocation baseline and the detailed design phase forms the product baseline. Each baseline is a management control point of systems engineering (MIL-STD-499B, 1994).

3.2.4.2 Implementation of Systems Engineering Process

Systems engineering conducts the management through a technical engineering process to give an effective solution to the problems that are required for the successful development of a system. The technical engineering process can apply to all stages of the design and development; its major functions are described below (Daup, 2001).

Systems engineering process takes the following three roles of:

- Transforming system requirements into the system design solutions and process descriptions;
- Producing information and resources required for decision making, and;
- Providing input for the next design and development phase.

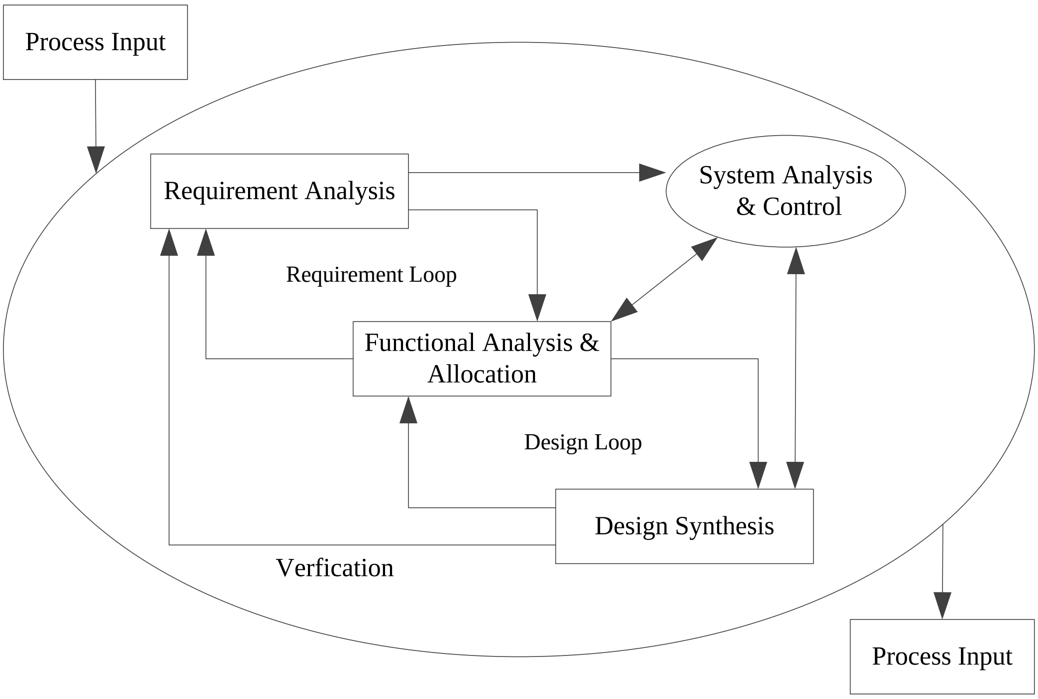


Figure 3.4 Systems Engineering Process (From MIL-STD-499B, 1994)

There are many kinds of systems engineering process models in the different international standards (for example, MIL-STD-499B, EIA 632, IEEE 1220, ISO/IEC 15288 etc.) and literature. Figure 3.4 describes a process model, published as a military standard of MIL-STD-499B (1994). The systems engineering process has basic three functions: (1) requirement analysis, (2) functional analysis and allocation and (3) design synthesis. Each process phase is conducted through the activities of definition, identification, analysis, evaluation, control and verification as shown in Figure 3.4.

The process is iteratively implemented by two process loops, such as requirement loop and design loop. Each process phase includes the verification or validation activities to verify the successful achievement of input as illustrated in Figure 3.4. The detailed description of the systems engineering process and its activities will be provided in Chapter 4.

3.2.4.3 Integration of Life Cycle Functions

Another role of the systems engineering management is to integrate all functions required throughout the entire life cycle period of a system into the systems engineering process to resolve effectively all possible problems that may be caused in the system life cycle period. Daup (2001) provides the eight primary functions of the system life cycle to be integrated into the systems engineering process. The eight primary functions of the system life cycle are: (1) design and development, (2) manufacturing, (3) deployment, (4) operation, (5) support, (6) disposal, (7) training and (8) verification.

3.2.5 Evolution of Systems Engineering Standards

There are many systems engineering standards, which have developed in the military and commercial sectors. Due to the development of many systems engineering standards, system engineers may sometimes have a difficulty when selects a useful standard as the basis for the design and development of a system.

Systems engineering standard was first developed and published by the US Military. After the first standard, “MIL-STD- 499 (1969) – Engineering Management,” was published by the US Military, several standards were developed in the commercial areas as described in Figure 3.5. The first standard was twice revised in 1974 (MIL-STD-499A) and 1994 (MIL-STD-499B). However, the MIL-STD-499B was revised in 1994, but it was not formally published. However, the principle and concept of the MIL-STD-499B were succeeded by the following three commercial standards: IEEE-1220 (1995), EIA 632 (1998), and EIA/IS-632 (1999) as depicted in Figure 3.5. Recently, the EIA/IS-632 and IEEE 1220 have been harmonized as a single concept, based on the ISO/IEC 15288 (2008) (Shead et al., 1994, 2001; Martin, 1998; EIA, 1994).

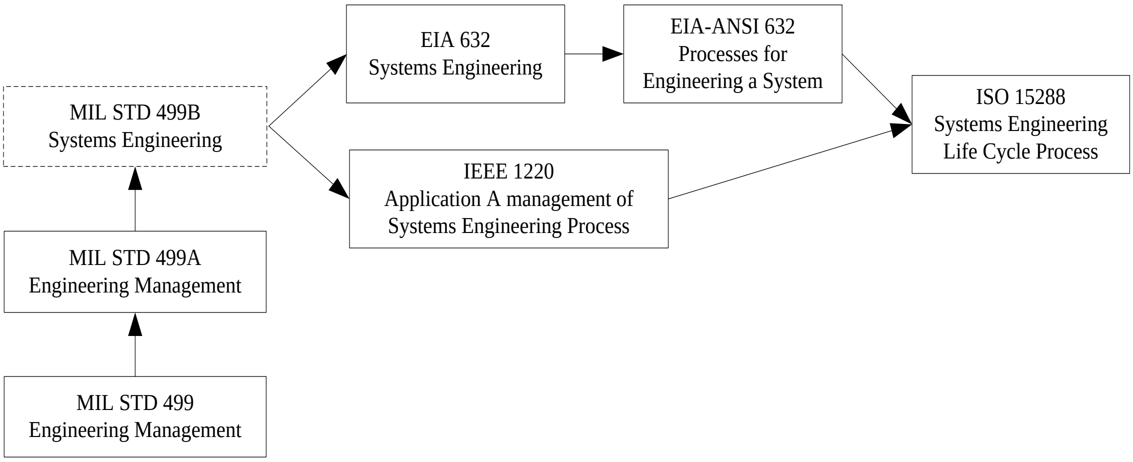


Figure 3.5 Evolution of Systems Engineering Standards

3.3. Concept of Systems RAMS Management

3.3.1 History of Systems RAMS Management

Systems RAMS is an enlarged engineering discipline that was originated from the concepts of safety and reliability. The concept of reliability and safety were firstly introduced by the aerospace industry in the 1930s. Due to the application of the statistical techniques in the system failure analysis, the safety and reliability became a significant engineering discipline of the aerospace system in the 1950s (An, 2005; Ebeling, 2010).

The safety and reliability engineering were introduced to assess product failure and human errors. 'Failure Mode and Effect Analysis (FMEA)' is the first technique for reliability and safety assessment, developed in the 1940s. The Boeing Company further updated the FMEA in the 1960s as 'Failure Mode, Effect, and Criticality Analysis (FMECA)' added 'Criticality analysis (CA)'. The CA reinforces the quantitative safety assessment through the analysis of single point failures, which directly affect systems safety (Nicholls, 2005).

In the 1970s, many advanced assessment techniques related to safety and reliability risk were developed in the aeronautical field, such as 'Event Tree Analysis (ETA)', 'Fault Tree Analysis (FTA)' and 'Probabilistic Risk Analysis (PRA)'. These techniques have been variously applied to many different industries, for instance, oil and gas, chemicals, railway etc. (An, 2005; Ericson, 2005).

Systems RAMS management has been adopted with the introduction of availability and maintainability concepts for safety and reliability, and the development of systems engineering since the early 1980s; it is achieved through the definition, assessment and control of all hazards that adversely affect the whole system, especially it was applied to the mission and safety critical systems. The systems RAMS management has developed as a distinct discipline of systems engineering since the early 1990s; it requires the established engineering concepts, methods, techniques, measurable parameters and mathematical tools (Villemeur, 1992; BS EN 50126-1, 1999).

In particular, railway organisations have applied RAMS management to achieve the systems safety, availability and cost-effectiveness in the management aspect of system's long term operation. The application of RAMS managment for railway systems engineering has been started from the US railway industry since the early 1980s, while the European railway has been applied it since the early 1990s, with the alteration of the contract scheme due to the introduction of systems engineering to railway project (BS EN 50126-1, 1999; Krri, 2007).

Railway RAMS management was firstly standardised by the European Committee for Electrical Standardisation (CENELEC) in 1999. The standard was subsequently adopted as an international standard, IEC 62278, of railway RAMS management in 2002, and its family standards: BS EN 50128 (2009) and BS EN 50129 (2003), were also published by the CENELEC. These standards have played a great important role in many global railway projects (BS EN 50126-1, 1999; Krri, 2007).

3.3.2 Definition of Systems RAMS Management

BS EN 50126-1 (1999) and Ucla et al. (2000) define systems RAMS management in the following three aspects as shown in Figure 3.6: (1) the definition of four RAMS characteristics to achieve RAMS requirements and operational contexts, (2) the assessment and control of all potential threats which adversely affect the achievements of RAMS requirements and (3) the provision of the means to achieve the systems RAMS requirements.

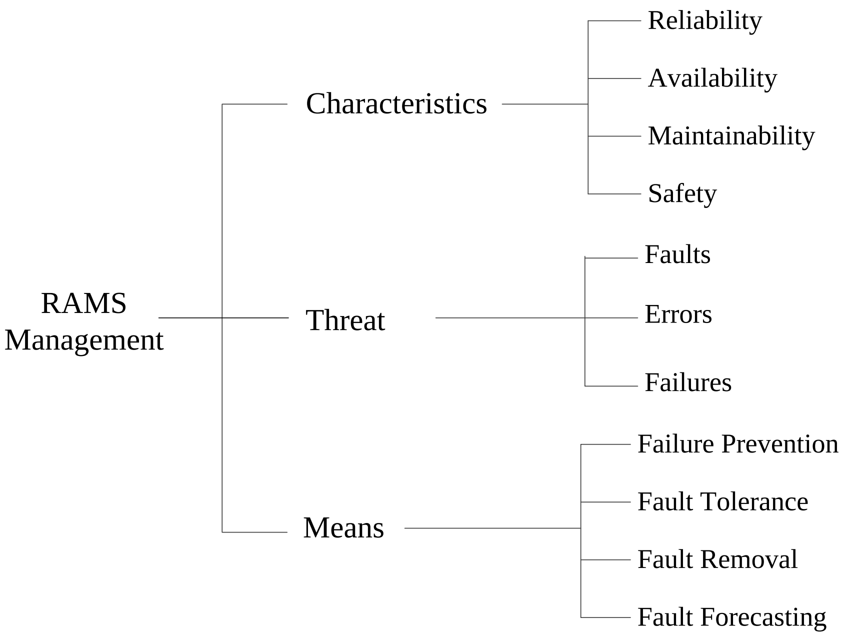


Figure 3.6 Concept of Systems RAMS Management (From Ucla et al., 2000)

Systems RAMS management defines four characteristics: reliability, availability, maintainability and safety as an inherent system product design property to ensure the successful accomplishment of the operational objectives of system. BS EN 50126-1 (1999) and Milutinović and Lucanin (2005) provide the general interrelation between systems RAMS characteristics under the operational objectives as shown in Figure 3.7.

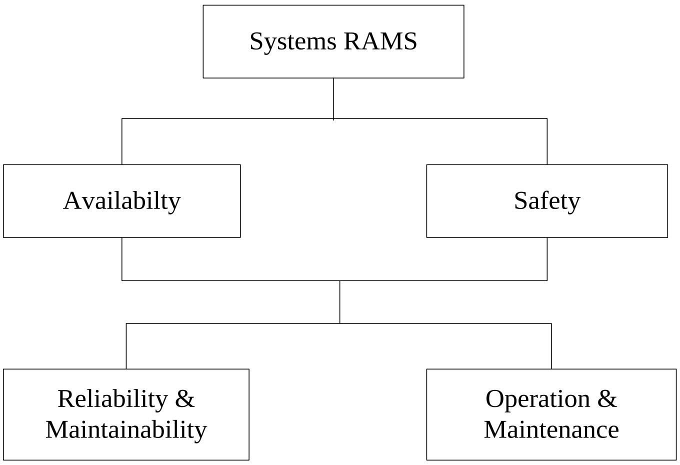


Figure 3.7 Systems RAMS Element Framework (From Milutinović and Lucanin, 2005)

Reliability characteristic represents the ability that a system can perform its intended function over a given time without any defined failure. Maintainability is a system characteristic that designs the ease of maintenance within the structure of a system. Availability characteristic means the ability to operate a system at the starting point of the required mission whenever required by operator. Finally, safety is a system design characteristic to provide freedom from unacceptable risks with regard to operation, maintenance, person, environment and equipment. The reliability and maintainability characteristics are determined by the system or operational availability and/or safety requirements as product design performance characteristics, while the availability and safety are achieved by the reliability and maintainability characteristics as shown in Figure 3.7 (Milutinović and Lucanin, 2005).

Systems RAMS management defines, assesses and controls all potential threats to a system: such as faults, errors and failures. The potential threats may occur from three sources, such as, system, operation and maintenance conditions. These factors are applied as an important input of RAMS management process, together with their effects, especially the input for their risk assessment (BS EN 50126-1, 1999; Lundteigen et al., 2009).

Systems RAMS management finally provides the means for the management, such as fault prevention, fault tolerance, fault removal and fault forecasting, as shown in Figure 3.6, in order to achieve the intended operational objectives. The means directly relates to the control of the threatening factors affecting the RAMS performance. Railway RAMS management in EN BS 50126-1 (1999) are based on the concept of precautions to minimize the possibility of impairment. The precaution is a combination of prevention and protection, but the prevention should be preferred to the protection in the RAMS management of a railway system (BS EN 50126-1, 1999).

Systems RAMS management is a process that implements the followings: (1) the informed decision of strategic direction of RAMS management policy, (2) the effective control of RAMS management functions and (3) the coordination of all RAMS management activities. The RAMS management is also performed, based on cost effectiveness, system effectiveness, risk and environmental impacts and project. The RAMS management of railway system will be discussed in detail in Chapters 4 and 5 (Vintr et al., 2007; BS ISO/IEC 26702, 2007).

For the effective systems engineering, railway RAMS management supports the following five activities (BS EN 50126-1, 1999; Lundteigen et al., 2009):

- Defining RAMS requirements;
- Assessing and controlling all threats to railway RAMS;
- Planning and implementing RAMS tasks;
- Achieving the compliance of RAMS requirements and;
- Conducting on-going monitoring and review.

3.3.3 Systems RAMS Risk Assessment

As mentioned above, risk assessment is a core part of RAMS management as well as systems engineering (BS EN 50126-1, 1999). Therefore, this section reviews the concept of systems risk and its risk assessment.

3.3.3.1 Definition of Risk

Risk is defined by the consequence of a hazard (or a failure mode). Risk assessment is a basis for implementing RAMS management and a core part of the RAMS management process (BS EN 50126-1, 1999):

Below are two definitions for the risk:

- "Risk is the combination of two elements of the expected frequency of occurrence of consequence (loss) of a hazard and the degree (severity) of the consequence." (BS EN 50126-1, 1999).
- "Risk is the likelihood that a hazard will actually cause its adverse effects, together with a measure of the effects." (Chen, 2012).

In general, the following basic four elements are required to define risk qualitatively and quantitatively. Figure 3.8 describes the relationship of these four elements (BS EN 31010, 2008):

- A potential root hazard causes (or failure causes);
- A hazard (or a failure mode);
- consequences (or failure effects) and;
- A probability of occurrence (or failure consequences).

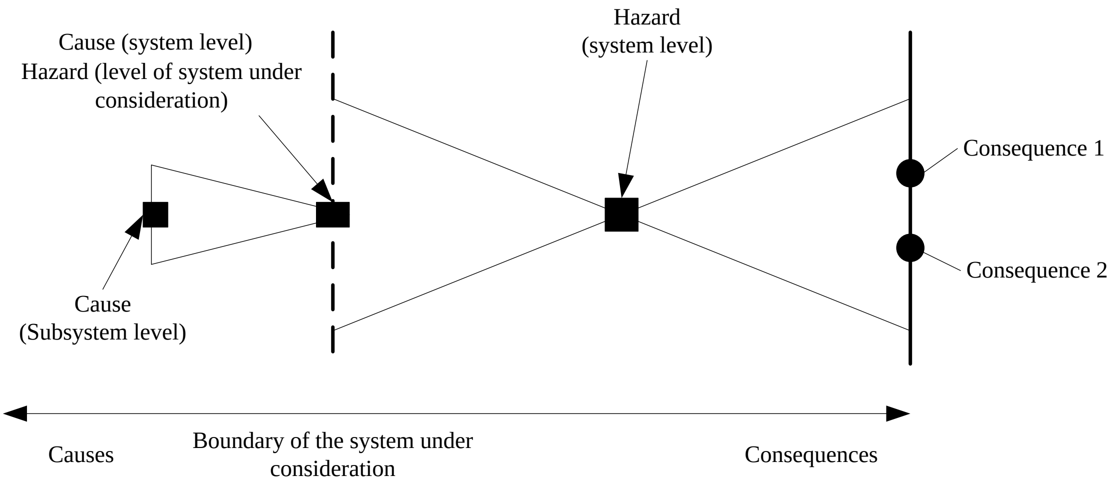


Figure 3.8 Concepts for Risk Definition (From BS EN 50129, 2003)

3.3.3.2 Definition of Risk Assessment

Risk assessment is a process that defines, identifies, analyses and evaluates a risk qualitatively, quantitatively and/or both. The risk assessment generally attempts to answer the following four fundamental questions (Chen, 2012; BS EN 31010, 2008):

- What can happen and why (by identifying risk)?
- What are the failure effects (by defining severity of the consequence)?
- How likely is it to happen (by defining frequency of occurrence of a failure)?
- What is the level of risk? Is the risk tolerable or acceptable and is any further control required (by applying risk assessment techniques)?

In order to answer the above questions, a system must be examined to define, identify, analyse and evaluate all potential hazards and their situations by a process as described in Figure 3.9 (An, 2005).

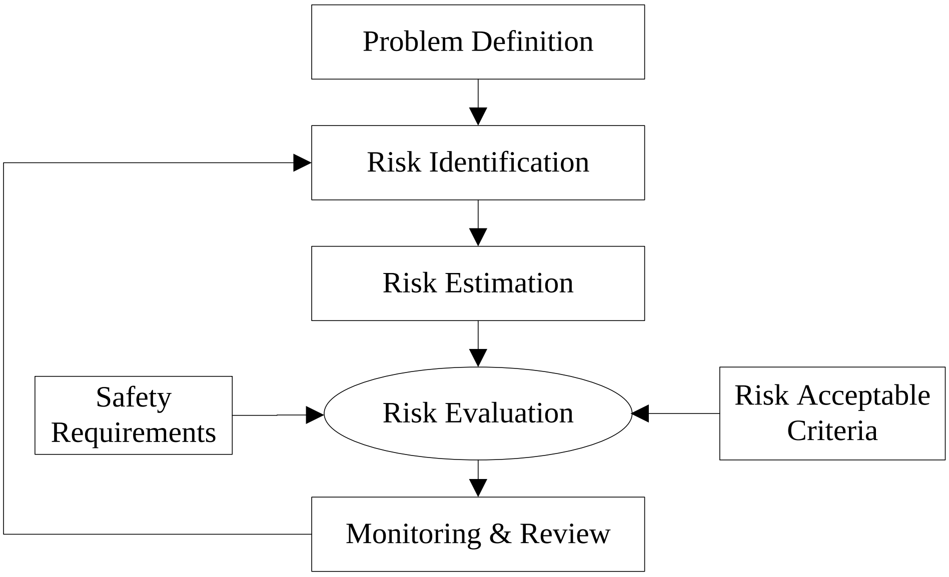


Figure 3.9 Risk Assessment Process (From An, 2005)

Risk assessment provides a comprehensive understanding for risks, and their causes, consequences and likelihoods (or probabilities) to support the decision making of systems RAMS management. The risk assessment also provides the following five factors to ensure the successful implementation of RAMS management (BS EN 31010, 2008):

- Selection between various options with different risks;
- Determination of risk priorities for decision making of risk management options;
- Selection of appropriate risk management strategies;
- Determination of the risk activity to undertake and;
- Determination of the risk levels to be controlled.

3.3.4 Risk Assessment Methods

Risk assessment fulfils the purpose of the intended risk assessment and the determination of the risk level of details required through the use of the information, data and resources that are collected. The risk assessment method can be classified into two groups: general and specific group. The general group can fall into three broad categories: qualitative, quantitative and semi-quantitative assessment by the analytical circumstances, data and resources. The specific group can be categorised by the analytical directions of the system design process, which are top-down and bottom-up assessment. The top-down assessment can be applied in the functional design phase and the bottom-up assessment can be applied for the physical product design stage (An, 2005; BS ISO 13824, 2008; BS EN 31010, 2008).

3.3.4.1 General Risk Assessment Methods

In the design phase of systems engineering, qualitative assessment methods are often used as a preliminary risk assessment to obtain the general level of the identified risk, and to identify and estimate all of possible potential risks. However, the qualitative assessment may be a necessary phase to undertake a semi-quantitative or complete quantitative risk assessment of the risks identified in each design process phase of systems engineering. For example, FMEA is a representative technique for the qualitative risk assessment (An, 2005; BS EN 60300-3-1, 2004).

A qualitative assessment is suitable for identifying all of possible failure effects and suggesting safety monitoring and safety functions in the functional (subsystem) design phase. Such a qualitative approach, instead of using quantitative data, may use some linguistic ranges to evaluate the frequency and the severity of the failure consequences. In general, four ranges, for example 'catastrophic, critical, marginal and negligible', may be generally used to classify the failure severity, and five ranges, for example, 'frequent, probable, occasional, remote and improbable', can be applied for the failure frequency (An et al., 2006; MIL-STD-882D, 2000).

A semi-quantitative risk assessment is very similar to the above qualitative assessment method, but a more expanded ranking scale can be applied, compared to the qualitative assessment. It includes most of the advantages of the quantitative methods. However, such an approach may be not as accurate as quantitative methods. If complete quantitative value is not available, the index parameters using risk assessment metrics, such as FMECA to transform the qualitative concepts into quantitative measures, can be applied. FMECA is a representative semi-quantitative risk assessment method (An et al., 2002; Chen, 2012).

A quantitative risk assessment method aims to provide system and RAMS designers with the quantified measures to determine the alternatives of a system design solutions. The quantified values have great advantages in applying, understanding and comparing risks. However, the quantitative assessment method requires the data and techniques for the statistical analysis.

The application of the quantitative method requires the deeper understanding for the system to design and the more detailed information that can further improve the system design. Fault tree analysis (FTA) and Event tree analysis (ETA) are the representative techniques of the quantitative risk assessment (An et al., 2011).

3.3.4.2 Specific Risk Assessment Methods

The top-down and bottom-up risk assessment methods are applied to identify and analyse the consequence scenarios of failure effect. The selection of the method is dependent on the data and information available, the indenture level of risk assessment, the complexity of the interrelation of the components and subsystems comprising the system to assess, and the level of the system's technical innovation (BS EN 60300-3-4, 2008; BS EN 31010, 2008).

Figure 3.10 is a top-down risk assessment process that identifies the root failure causes from the past failure data, whilst the further continued risk assessment for the intended lower level is required to define the hierarchy of failure causes. The top-down risk assessment is continued until all root failure causes are completely identified. Both the qualitative and quantitative risk assessment can be applied to this top-down assessment, but it requires the deeper knowledge and many experiences for risk assessment. FTA is a typical top-down risk assessment method (An, 2005; BS EN 60300-3-4, 2008; Chen 2012).

A bottom-up approach for the risk assessment is described in Figure 3.11. It is an inductive risk assessment method, which requires the detailed breakdown of a system to identify all possible failure modes. The failure modes are identified from the bottom level to the top level, and then the severity evaluation for the failure consequence and its frequency evaluation of occurrence are undertaken. The bottom-up risk assessment has the following features, compared with the top-down assessment (An, 2005):

- It can analyse precise failure modes and their causes;
- It is easier to use a computer package, and;
- It is appropriate for the risk assessment of the large, complex scale systems.

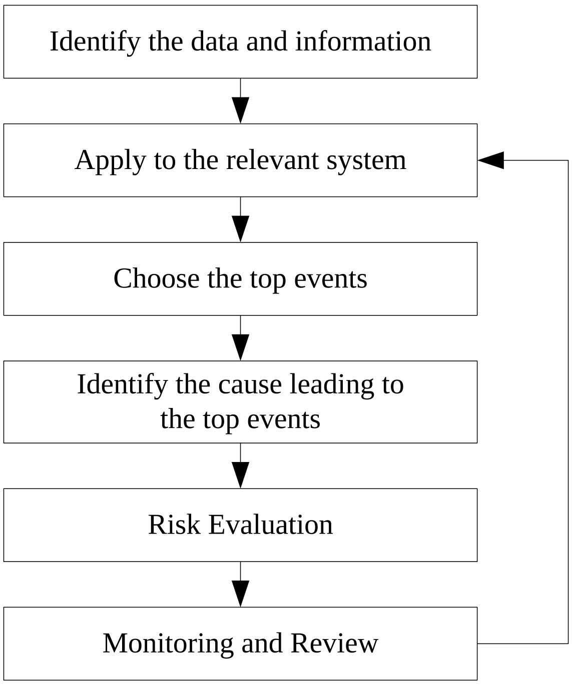

Identify the data and information
Apply to the relevant system
Choose the top events
Identify the cause leading to the top events
Risk Evaluation
Monitoring and Review

Figure 3.10 A Top-down Risk Assessment Process (From An, 2005)

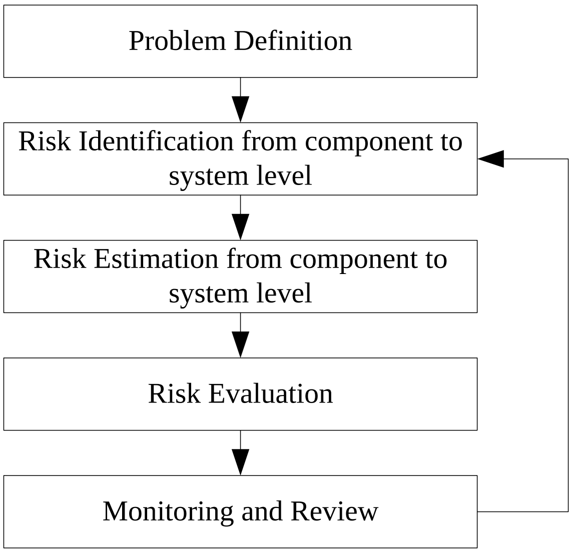

Problem Definition
Risk Identification from component to system level
Risk Estimation from component to system level
Risk Evaluation
Monitoring and Review

Figure 3.11 A Bottom-up Risk Assessment Process (From An, 2005)

3.3.4.3 Data Collection for Risk Assessment

Data for risk assessment can be obtained from appropriate information sources. The most common information sources and types can be used to estimate risk probability. The information can be collected from the following sources (BS EN 31010, 2008):

- Past failure/accident records (field data);
- Practice and relevant data (incident data);
- Experiments and prototypes;
- Engineering or other models, and;
- Specialist and expert judgement (expert opinion).

3.3.4.4 Selection of Risk Assessment Technique

BS EN 31010 (2008) and BS EN 60300-3-4 (2008) provide the methods that select risk assessment technique in the following two aspects: risk assessment process phase and factors affecting risk level. Tables 3.2 and Table 3.3 are summarised for the results estimated for the eight typical risk assessment techniques and they are referred from BS EN 31010 (2008) and BS EN 60300-3-4 (2008). Table 3.2 provides the applicability of the typical risk assessment techniques in the risk assessment process. Table 3.3 explains that of the typical techniques by the three factors affecting the risk level of a system.

Table 3.2 Estimation of Typical Risk Assessment Techniques in Risk Assessment Process

Types	Risk Assessment Process				
	Risk Identification	Risk Analysis			Risk Evaluation
		Consequence	Likelihood	Level of Risk	
FMEA[3]	SA	SA	NA	NA	NA
FMECA[4]	SA	SA	SA	SA	SA
FTA[5]	NA	A	A	A	A
HAZOP[6]	SA	SA	NA	NA	SA
RCM[7]	SA	SA	SA	SA	SA
PHA[8]	SA	NA	NA	NA	NA
ETA[9]	NA	SA	SA	A	NA
RBD[10]	SA	A	A	A	A

❖ NA: Not Available; SA: Selection Available; A: Available

Table 3.3 Estimation of Typical Risk Assessment Techniques by Risk Influence Factors

Techniques	Relevance of influence factors			Quantitative Output
	Resources & Capacity	Nature & Degree of Uncertainty	Complexity	
FMEA	Medium	Medium	Medium	+
FMECA	Medium	Medium	Medium	+
FTA	High	High	High	++
HAZOP	Medium	High	High	+
RCM	Medium	Medium	Medium	++
PHA	Low	High	Medium	±
ETA	Medium	Medium	Medium	++
RBD	High	High	High	++

❖ ++: Excellent; +: Good; ±: Possible

[3] Failure Mode and Effect Analysis
[4] Failure Mode, Effect and Criticality Analysis
[5] Fault Tree Analysis
[6] Hazard and Operability Study
[7] Reliability Centred Analysis
[8] Preliminary Hazard Analysis
[9] Event Tree Analysis
[10] Reliability Block Diagram

3.3.4.5 Difficulty in Risk Assessment

Many risk assessment techniques have been developed and they have applied in many different industries. However, there are several difficulties regarding the application of risk assessment method and technique in the systems engineering design phase. An (2005) provides several difficulties of risk assessment as follows:

- The collection of resources, data and information available are highly limited and they are statistically inaccurate;
- Many threats affecting system performance have difficulty in implementing the mathematical modelling to assess system's functional behaviour;
- The quantitative risk assessment is essential in the system design analysis, but it is expensive and it also requires accurate data. Hence, determining the scope and depth of risk assessment is very difficult;
- The quantitative risk assessment of failure consequence can involve great uncertainty due to inaccurate data, and;
- The qualitative assessment requires many analytical experiences with numerous assumptions, estimations, opinions and judgments, but the assessment results may often be subjective, depending on the analysts.

3.3.5 RAMS Management Standards

Railway RAMS standards have been developed based on BS IEC 61508 series (2002 and 2005) as shown in Figure 3.12. The BS IEC 61508 series are the representative standards for safety management related to the electrical/electronic systems.

Three railway RAMS management standards were developed by the CENELEC and they are based on the BS IEC 61508 series as shown in Figure 3.12. BS EN 50126-1 was first published in 1999 as the basic principle and application of railway RAMS management. BS EN 50128 is a standard for the software RAMS management of communication, signalling and processing systems involved a railway system and it was developed in 2008. BS EN 50129 is a standard related to the hardware RAMS management of railway signalling system and it was published in 2003. These RAMS management standards have been revised every five year (Lundteigen et al., 2009; Nordland, 2003; Braband et al., 2003; Pasquale, 2003).

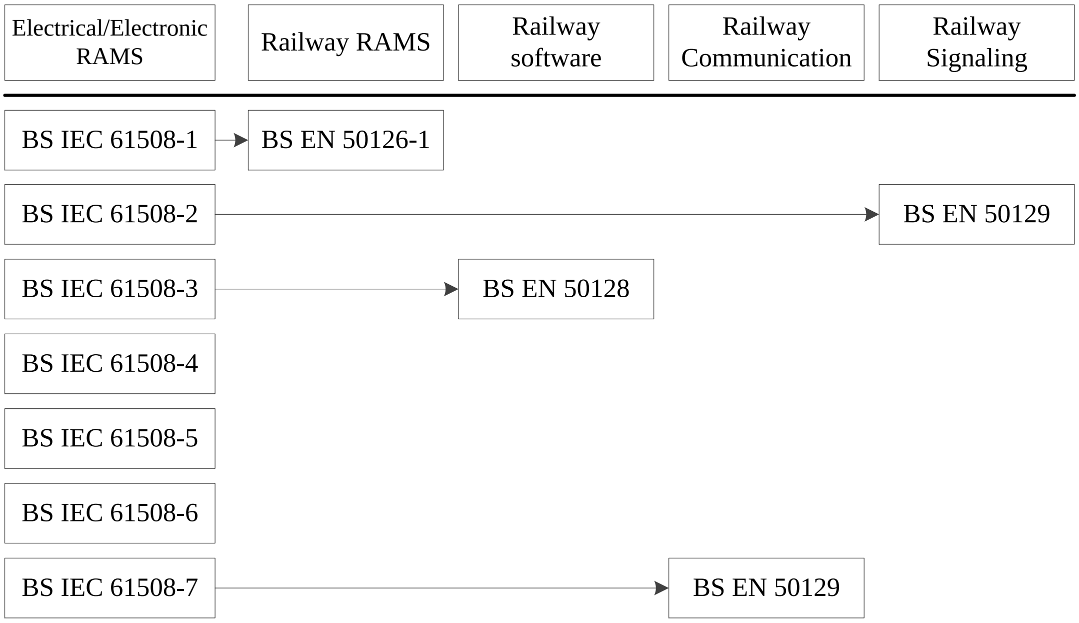


Figure 3.12 Railway RAMS management Standards

3.4 Techniques for RAMS Management

This section reviews several important RAMS management techniques, which have been developed to support RAMS management process effectively.

3.4.1 Functional Analysis

Functional analysis (FA) is an essential technique to understand and design the desired system performance and critical functions. It is necessary to perform the FA in the RAMS management and systems engineering. Therefore, FA is the basis and starting point of the risk assessment and RAMS management to analyse the functional behaviours. The objective of the functional analysis is to provide the main information that affects the system function and performance and to establish a fundamental basis for RAMS management. The FA is also used for specification, modelling, simulation, validation and verification. Accordingly, FA is often used as an important design tool to define a system's functional structure. The functional analysis generally uses the following two ways:

- Structured Analysis and Design Technique (SADT);
- Functional Analysis System Technique (FAST).

SADT has been used in many industrial fields. It is a diagrammatic notion designed to understand and describe system's functional behaviours and interfaces. It offers the building blocks to represent data flow and activities, and a variety of arrows related to the building blocks as shown in Figure 3.13, which is an example of SADT (Rafrafi et al., 2006).

FAST was developed by Charles Bytheway in 1964; it is also used in many industrial areas. The FAST can be utilised in the situations that can be functionally represented to depict the functions in a logic sequence, to prioritise them and to test their dependency. It is not able to solve the functional problems, but it can identify the system's essential functional characteristics. Figure 3.14 is an example of FAST model developed by Kaufmnan (1982).

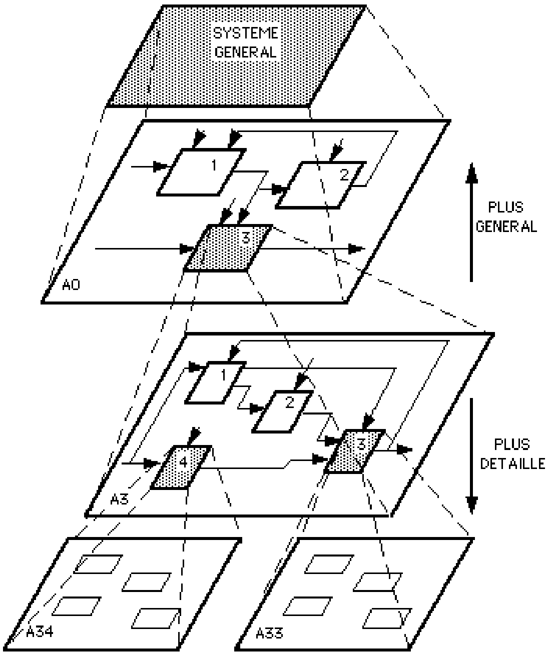


Figure 3.13 SADT Model (From Rafrafi et al., 2006)

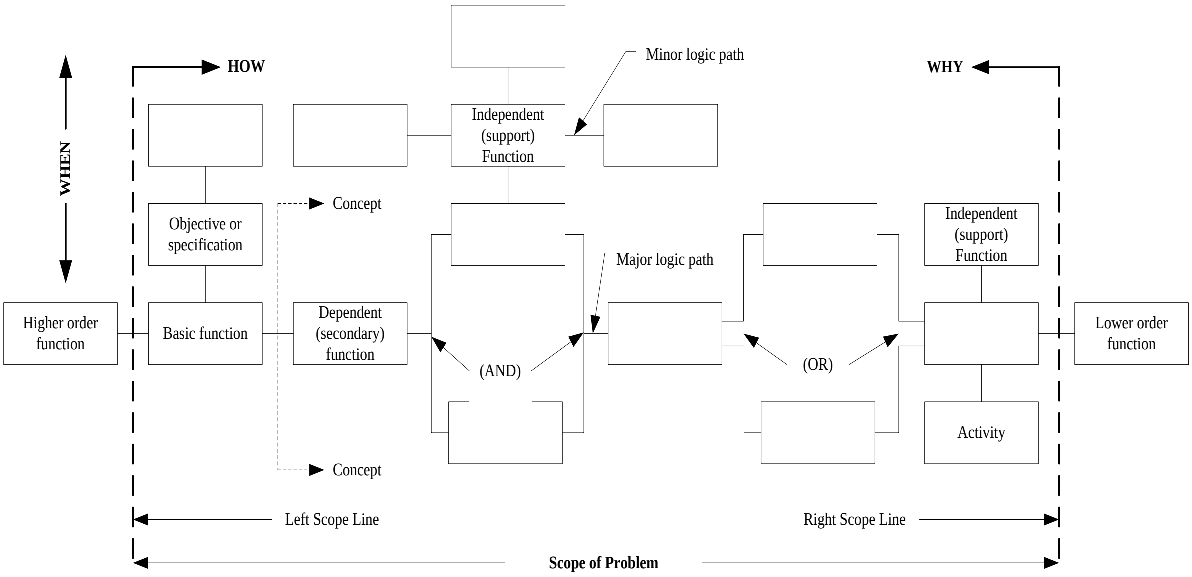


Figure 3.14 FAST Model (From Kaufmnan, 1982)

3.4.2 Preliminary Hazard Analysis

Preliminary Hazard Analysis (PHA) is a technique to assess the risks identified in the system level. The purpose of PHA is to identify all potential hazards possible, and their causal factors, effects and level of risks, and to control the identified hazards. The PHA is also intended to provide a process that assesses all possible hazards in the system definition phase and establishes the system requirements through the results of the PHA. Several modified PHA are sometimes used under different names, such as rapid risk ranking (RRR) and hazard identification (HAZID) (Ericson, 2005; BS ISO/IEC 26702, 2007).

PHA technique was originated by the US military in the 1960s for the safety risk assessment of missile system. Thereafter, it has been widely applied to many industrial fields. The PHA technique is generally used in the requirement analysis stage of the systems engineering process, namely after system boundary, interface and operational contexts are defined. The PHA was formally established and announced by the developers of MIL-STD-882 and it was orginally called a gross hazard analysis because it was conducted in the preliminary design phase (MIL-STD-882D, 2000).

PHA provides an initial overview of the risks that may appear in the overall functional behaviour of a system. It also provides a broad risk assessment, which is usually not detailed or specific. However, PHA in the low risk systems is implemented for identification of total risks. On the other hand, in the high risk systems such as airplane and railway, the risk identified is prioritised to provide the full range of risk issues. The PHA can be applied to the concept design phase of a system as well as all subsystems and componets (Ericson, 2005; BS ISO/IEC 26702, 2007).

3.4.3 Failure Mode and Effect Analysis

Failure modes and effects analysis (FMEA) is a safety and reliability assessment technique to assess all potential failure modes and their failure effects of the components comprising a system, which may affect the entire system performance. It also identifies how to avoid the failure modes and how to reduce the impacts of the failure modes. The FMEA is a technique that defines, identifies, prioritises and controls all potential failure modes that may include in the system design and manufacture phases or their process (Kim at el., 2009; Nicholls, 2005).

Initially, FMEA was called FMECA. The 'C' in FMECA is an abbreviation for the criticality rank of the failure modes that are included in the system. However, FMEA is often regarded as a synonym for FMECA, but its function is completely different. In general, FMEA is used to rank the severity of the effects of a failure mode; whilst FMECA includes ranking the frequency of occurrence of the failure effects as well as their failure severity. The combination of the failure severity and frequency is called the criticality or risk of a system (MIL-STD-1629A, 1980).

FMECA was one of the systematic techniques for the failure analysis in the system design process and it is applied essentially as a core part of the system design process in the large, complex system project. FMECA was developed by the US military in the 1950s and the first guideline procedure 'Mil-P-1629' was published in the 1950s. FMECA is the most commonly and widely used reliability and safety assessment technique in the system concept design stage to ensure that all potential failure modes have been considered (Ebleing, 2010; Ericson, 2005).

FMECA can be used to determine the alternatives of the system design solutions with high reliability and safety risk at the conceptual design phase. It also guarantees that all possible failure modes and their effects related to the mission success of the system have been referred and listed. FMECA can develop the testing plan and the test acceptance criteria of the system requirements, and it can provide a basis for the plan, functions and activities of the system maintenance. Finally, FMECA can give the fundamentals for the RAMS assessment (MIL-STD-1629A, 1980; BS EN 60812, 2006).

The following six basic questions are required to perform FMECA effectively (Moubray, 2001):

- How can a system fail?
- What is the mechanism for the failure modes which occur?
- What is the consequence of a failure mode?
- What are the effects for the safety of a failure mode?
- How can the failure mode be detected?
- How can the design for a failure mode be supported?

FMECA can be performed by the two analytical approach methods: bottom-up and top-down approach. The bottom-up approach is used for making decisions on the concept of a system. It is applied from each component level to the overall system level. The bottom-up approach is sometimes called hardware approach. On the other hand, the top-down approach is mainly used in the functional analysis before making decisions regarding the whole system structure. The analysis is focused on the functions, and the functional failures with signficant effects are prioritised for selecting design solutions. Although the functional approach is not a complete analysis, it may be used for an existing system to identify the problem areas for making decisions on safety functions (BS ISO/IEC 26702, 2007).

In summary, FMECA is used for analysing: (1) Design FMECA, which is conducted to improve potential failure during the design process, considering all types of potential failures which may occur during the whole system life cycle, (2) Process FMECA, which is used for solving the problems which may occur in manufacture, maintenance or operation processes and finally (3) System FMECA, which looks for potential problems and weak points in larger processes.

There are many standards for FMECA analysis, such as MIL-STD-1629A (1980), BS IEC 60812 (2006) and SEA-J 1739 (1970), but their analysis methods are slightly different as shown in Figure 3.15. Table 3.4 summarise the major difference between the three standards in the application of failure mode to FMECA analysis. This research will apply the method of MIL-STD-1629A (1980) in terms of risk definition of Section 3.3.3 (Kim et al., 2009).

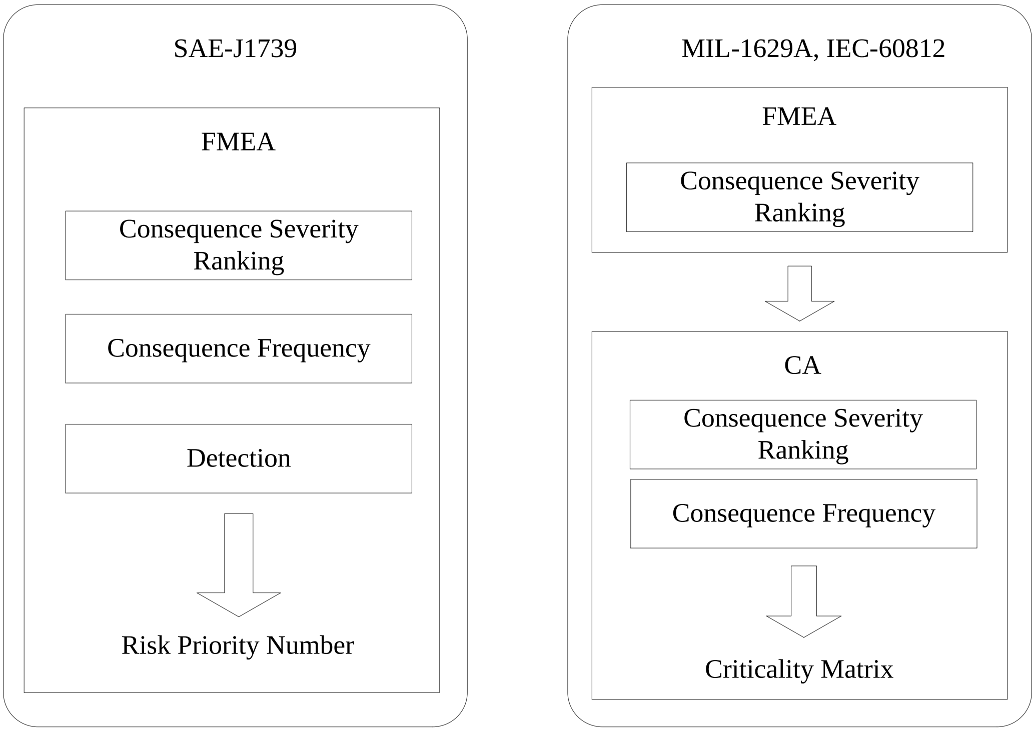


Figure 3.15 Analytical Differences of FMECA Standards

Table 3.4 Analytical Differences of FMECA Standards

	MIL-STD-1629A	BS EN 60812	SAE–J1739
Analysis Step	2 Levels (FMEA & CA)		1 Level (FMEA)
Criticality Analysis	Severity, Frequency		Severity, Frequency, Detection
Criticality	Criticality Ranking		RPN (Risk Priority Number)
Criticality Determination	Failure Mode		Failure Cause
Significance of Severity & Occurrence Frequency	Severity		Severity and Frequency are equal
Failure effect analysis	3 Levels (Local, Next & End level)	2 Levels (Local & End level)	1 Level (Failure Effect)

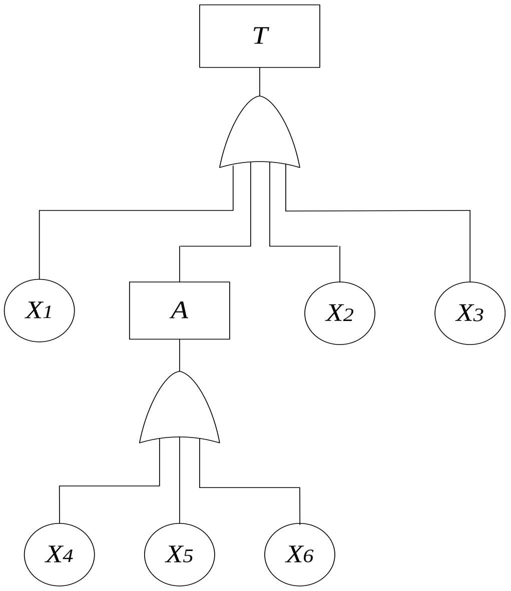
3.4.4 Fault Tree Analysis

Fault tree analysis (FTA) is a systematic, deductive and symbolic logic analytical technique to identify, model, analyse and evaluate the conditions and factors which may cause a fault event (or top event), and which may affect the system performance related to safety, reliability, maintainability and cost. FTA can be considered as one of the most reliable techniques to logically assess the reliability and safety assessment of a fault event (Stamatelatos and Caraballo, 2002; Ericson, 2005; Andrews, 2012).

FTA was developed by H. Watson and Allison B. Mearns in 1962, who together worked at the Laboratory of the US Bell Company, and the Boeing Company further applied the FTA technique to quantify the safety factors that affect the weapon systems. In addition, many industries such as the commercial aircraft industry (1960s), transportation (1990s), the chemical industry (1980s) and the nuclear power industry (1970s) have widely used the FTA technique for safety and reliability assessment (Ericson, 1999).

FTA focuses on a subset of all possible failure modes, in particular those that may cause catastrophic failure effects. The gate, events and cut sets are the major analytical elements of the FTA. The logical diagram, 'AND' and 'OR' gates, depicts the analytical results of the FTA. The failure effects show input into gates, and the cut sets represent a set of failure effects that can cause a system failure. FTA can be usually used as a combination of FMECA, Markov and Event Tree analysis (ETA) in order to overcome the limitations that FTA may have in the failure analysis (Stapelberg, 2008; BS EN 60812, 2006).

FTA can be applied to all process stages of the system engineering, as an analytical technique for effective improvement of potential design problems included due to incomplete information and data related to the design details in the concept design phases. The early analytical activities can be extended by the increased availability of information and data. FTA also identifies and assesses the potential problems that may be induced from product design, environment or operation, manufacturing and operational and maintenance conditions (Muttram, 2002; BS EN 61025, 2007).



T: Rolling stock derailment

A: Track fault

X_1 : Rolling stock faults

X_2 : Running into obstruction

X_3 : Over-speed

X_4 : Broken rail

X_5 : Bucked rail

X_6 : Track twist

Figure 3.16 A Fault Tree Example for Rolling Stock Derailment (From Muttram, 2002).

Figure 3.16 depicts an example of FTA analysis on the derailment event of rolling stock. The top event of the fault tree is defined as “the derailment event of rolling stock” which is connected by one intermediate event (A) and three basic events (X_1, X_2, and X_3) by an OR gate. The intermediate event shows the main causes of the top event. The three basic events (X_4, X_5, and X_6) show the causes of track faults (Muttram, 2002).

3.4.5 Event Tree Analysis

Event Tree Analysis (ETA) is one of the techniques that estimate the sequence of failure events in the consequence scenario analysis of a potential failure event. ETA uses a graphical logic tree model, i.e., an event tree that represents a serious hazard, to determine whether the failure event is effectively controlled by the safety systems or not. ETA may bring about many possible outcomes from an initiating event. It can provide a probability for each outcome as shown in Figure 3.17 (Ericson, 2005; BS EN 62502, 2009).

ETA consists of a binary form of a decision tree in which multiple decision paths are determined as shown in Figure 3.17. ETA was published by the WASH-1400 in1974, which is a nuclear plant safety study. The WASH-1400 presented that the PRA[11] of a nuclear power plant could be described by the ETA; however, it would be very complex and large if it is constructed by the fault trees of FTA. The ETA was established as a useful technique that can condense the analysis into a more manageable picture, while still utilising the FTA (Ericson, 2005).

ETA is generally applicable for almost all types of risk assessment, but it is effectively used to model the accidents where multiple safeguards are in place as protective features. ETA is highly effective when it determines various initiating events for accidents of interest, as

[11] Probability Risk Assessment

shown in Figure 3.17. An event tree is started from the establishment of an initiating event, such as a component failure which is caused by the increase in temperature, pressure, or the release of a hazardous substance. The consequences of the events follow a series of possible paths. Each path can be allotted by a probability of occurrence through the application of FTA, and the probability of all possible outcomes can be calculated as shown in Figure 3.17 (Berrado et al., 2010; BS EN 60300-1, 2004)

Figure 3.17 shows an ETA model that analyses the failure consequence scenarios of an event. The failure scenarios can be represented by the FMEA and the failure probability also can be assessed from the FTA analysis. This model will be discussed in more detail in Chapter 5.

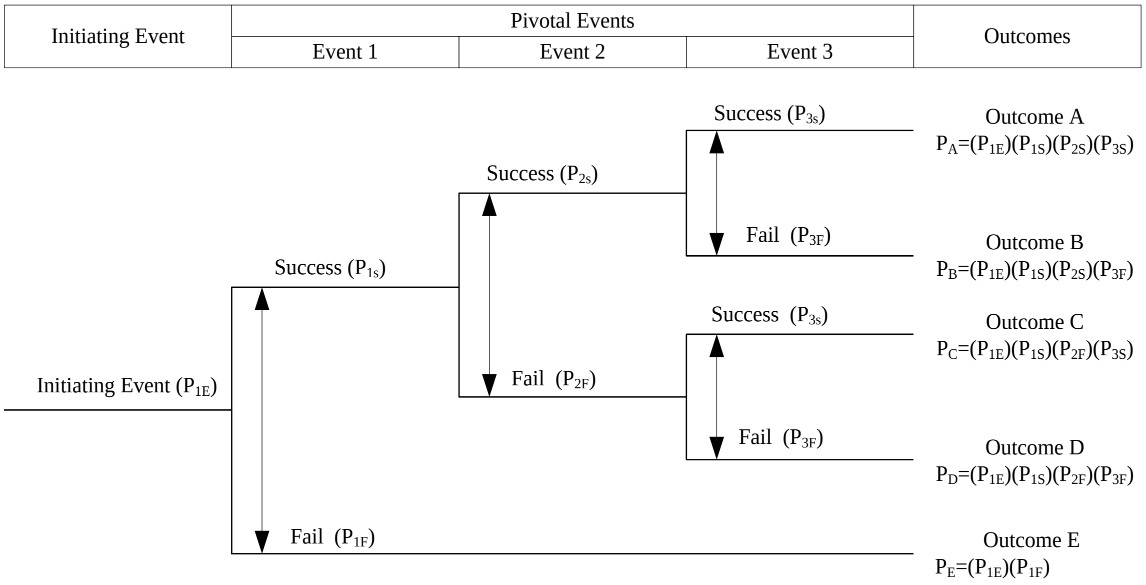


Figure 3.17 ETA Model (From Stapelberg, 2008)

3.4.6 Reliability Centred Maintenance

Reliability Centred Maintenance (RCM) is a logically structured maintenance analysis technique to identify and determine the failure management policies for the achievement of the operational objectives such as safety, availability and cost. The failure management policies generally include maintenance strategies, operational changes, design modifications or others to control the consequences of a failure mode. However, it focuses on the effective and economic maintenance policy to keep the safety and availability of a system (BS EN 60300-3-11, 2009; Moubray, 2001).

Until the early 1960s, all maintenance schemes, such as preventive maintenance, periodic replacement or overhaul, were planned and performed in terms of the constant interval, which were determined by the operational experience of the maintenance organisations. To resolve the problem, RCM programme was first developed by the commercial aviation industry, based on ATA MSG–3, which is an airline maintenance-planning document. RCM is now accepted in the wider industrial fields, such as aviation, the oil industry, railways, shipping etc., as a proven methodology for maintenance (Carretero at el., 2003; BS EN 50126-3, 2006).

RCM provides a structured logical decision process to determine appropriate preventive maintenance policies, design improvements, or alternatives appropriate to safety, operational consequences, and the degradation mechanism of potential functional failures, the analysis of which is supported by FMECA, FTA etc. The application of RCM at the design stage is generally the most effective, but RCM at the operation and maintenance stages can be applied for the improvement of the existing maintenance policy (BS EN 60300-3-11, 2009; Blanchard et al., 1995).

Figure 3.18 shows a RCM procedure that can be performed with FMECA in the system engineering design process. RCM is generally implemented to control the results of risk assessment by a preventive maintenance strategy.

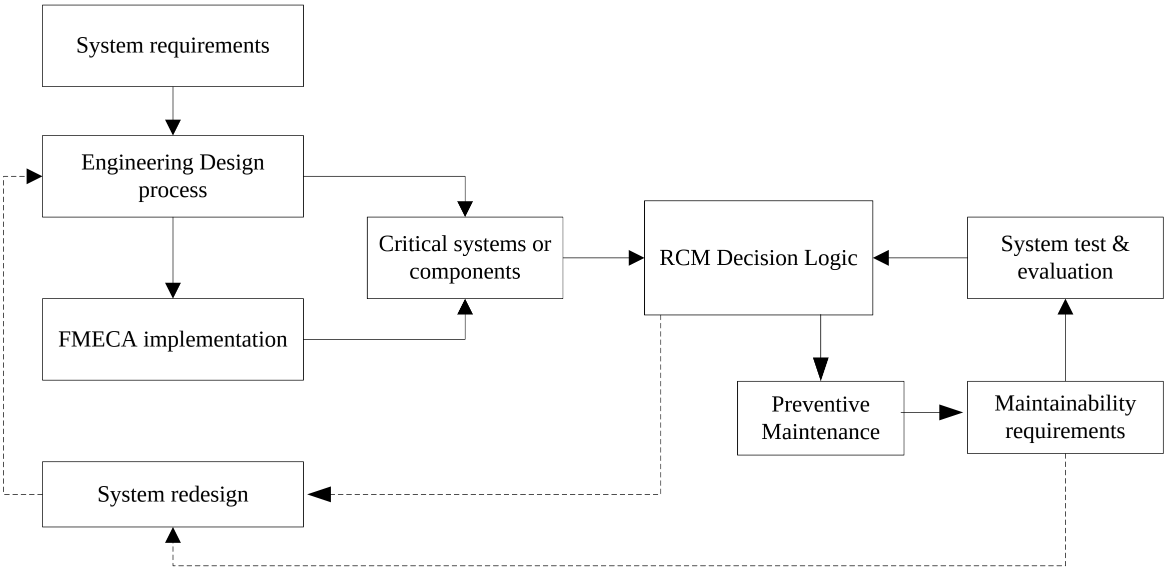


Figure 3.18 RCM Model (From Blanchard, 2012)

3.4.7 Hazard and Operability Study

Hazard and operability study (HAZOP) analysis is a systematic assessment technique that identifies and analyses potential hazards and operability problems of a system; it uses an organized, structured and methodical process (Ericson, 2005; Berrado et al., 2010).

The Chemical Industry Institute of the United Kingdom formalized the HAZOP in the 1970s. It is widely used in many safety critical industries as well as the chemical industry. Herbert. G. Lawley firstly published the paper on the HAZOP technique in 1974 to give a guideline on how to use HAZOP in practice of hazard assessment (Ericson, 2005; BS IEC 61882, 2001).

The HAZOP deploys several guidewords to help the analysts find what is deviated from the system design objective. The design deviations are identified by a questioning process using the guide words: ‘No or Not’, ‘More’, ‘Less’, ‘As well as’, ‘Part of’, ‘Reverse’, ‘Other than’ etc. as shown in Table 3.5. The guidewords take the role of stimulating imaginative thinking to maximize the effectiveness of the study. HAZOP is most suitable after the detailed design phase in order to investigate operating problems. Table 3.5 shows an example of the application of HAZOP for analysing the operational problems of train doors at platforms (BS IEC 61882, 2001; BS EN 60300-3-1, 2004; Choi, 2008).

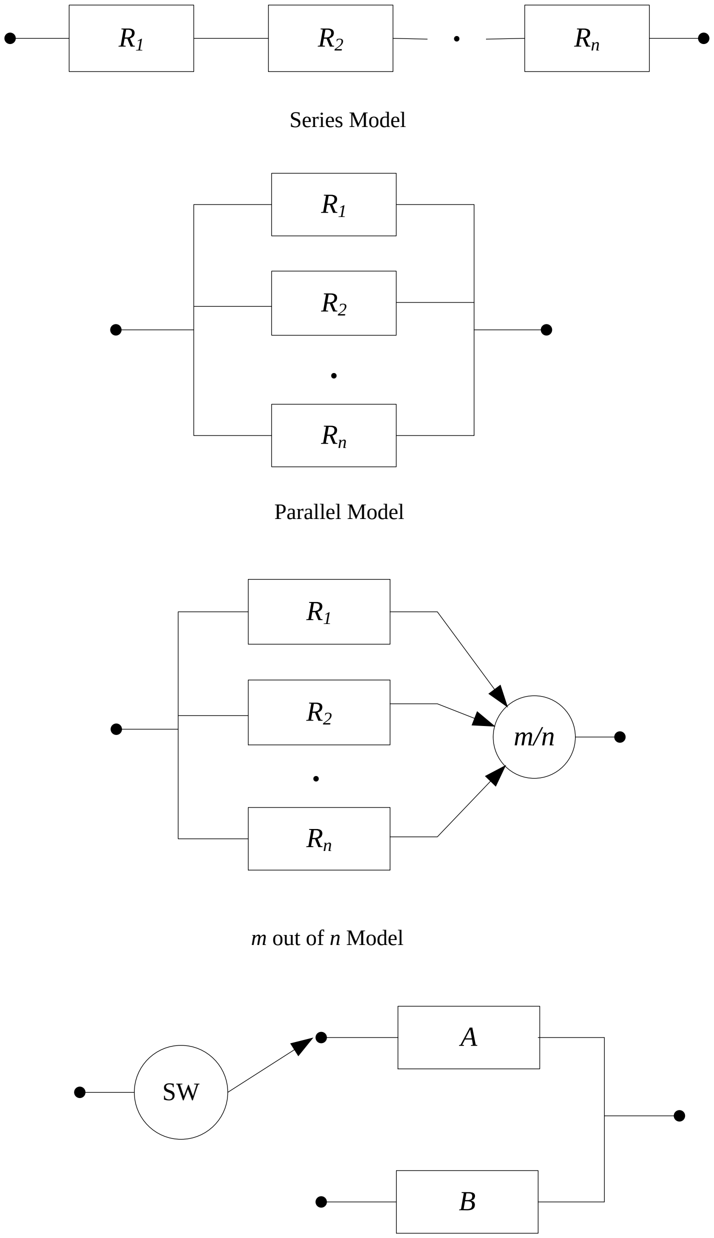
Table 3.5 An example of the application of HAZOP (From Choi, 2008)

Guideword	Deviation	Cause	Effect
No	Doors fail to open	Defective mechanism	No passenger egress
More	Doors open too early (train moving or not adjacent to platform)	Operator error	Possible harm to passsengers
Less	Only one door open	Defective mechanism	Restricted passenger egress, may lead to crush injuries
As well as	Doors open on both sides of train	Failure in control circuitry	Possible harm to passengers if they exit the wrong door
Part of	Same as less	-	-
Reverse	N/A	N/A	
Other than	Doors open wrong side	Failure in control circuitry	Possible harm to passengers if they exit the wrong door

3.4.8 Reliability Block Diagram

Reliability block diagram (RBD) is a graphical analysis technique to represent the reliability of the system structure that is logically connected. The blocks of RBD represent the system success paths, which is made in various different levels for the use of qualitative analysis (e.g., FMEA, FTA etc.) and quantitative analysis (e.g., simple Boolean algebra techniques for analysing minimal cut sets and path sets) (BS EN 61078, 2006; BS EN 600300-3-1, 2004).

RBD is directly built from the system functional diagram and systematically represents the functional paths. It can express many different types of system configurations, for example, series, parallel, redundant, standby etc. as shown in Figure 3.19. The RBD is used to analyse variations and trade-offs of system performance parameters and set up models for reliability and availability evaluation. However, the RBD is not used for a specific fault analysis such as the cause and effect analysis and applied probabilistic models of system performance. Figure 3.19 shows examples of RBD models for reliability design and assessment (BS EN 61078, 2006; Berrado et al., 2010).



Series Model

Parallel Model

m out of *n* Model

Standby Redundancy Model

Figure 3.19 RBD Models (From BS EN 61078, 2006)

3.4.9 Fuzzy Logic Analysis

A fuzzy set (FS) is a theory that can effectively solve problems that are inaccurately defined and insufficiently handled information by means of a method which reinforces the cognitive of expert systems and controls uncertainty. The FS provides an excellent tool for decision making in a conflicting management environment. It can be effectively integrated into the risk assessment process to obtain more reliable results from highly uncertain and ambiguous information (An, 2005; An et al., 2011).

The FS was developed by Lukasiewicz in the 1920s and Zadeh extended the FS into a formal system of mathematical fuzzy logic in 1969. It is a branch of logic which uses the degrees of membership in sets. Fuzzy logic defines the set of vague, linguistic terms: e.g., low risk, reasonable risk or high risk. These terms are not fixed with a single value, but FS theory provides the means by mathmatical logic (An et al., 2006).

The two dynamic techniques, i.e. Fuzzy decision function (FDF) and fuzzy inference (FI), are provided for decision making and modelling as shown in Figure 3.20. The FDF is a tool which combines decision objectives and constraints in order to confirm the decision maker's preferences. Linguistic rules provide interpretations and transparency for the FI. This desirable facility provides a mapping between inputs and ouputs described in the fuzzy rule-based system. A risk assessment model through the above two fuzzy techniques is shown in Figure 3.20 (An et al., 2006; An et al., 2011).

The proceeding steps of the new fuzzy risk assessment model are explained below (An, 2005):

Step 1: Investigate and check risk related data and information;

Step 2: Determine risk criteria;

Step 3: Measure risk criteria;

Step 4: Input the risk criteria into the FDF of two main actions: fuzzification and Aggregation;

Step 5: Input the aggregated criteria into the proposed FI system, and;

Step 6: Convert the fuzzy result into a matching crisp value (Defuzzification).

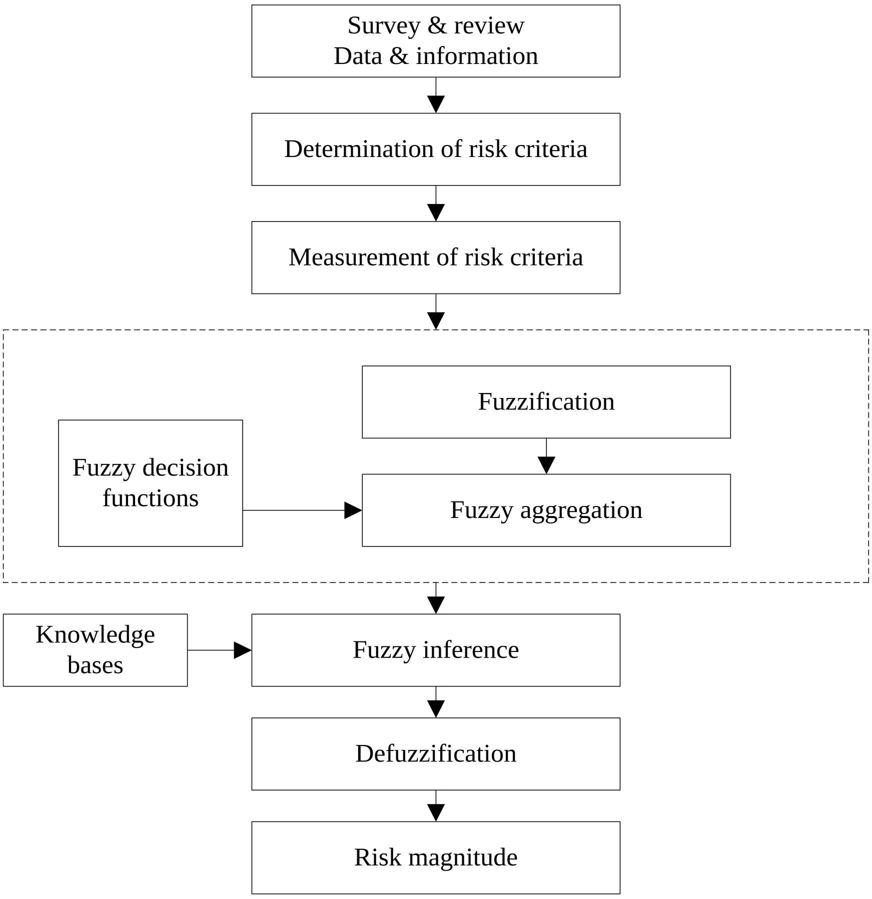


Figure 3.20 Fuzzy Logic Analysis Model (From An, 2005)

3.4.10 RAMS Requirement Allocation

The allocation of RAMS requirement is an essential part for design of the lower systems (i.e., subsystems) in the systems engineering process. The objective of the requirement allocation is to find the most effective physical design architecture that can achieve the RAMS requirements of the system level and the allocation is conducted by the analysis of the functional behaviours. When a RAMS design is required, an allocation of each performance characteristic for reliability, availability, maintainability and safety is necessary and the allocation techniques for four RAMS characteristics are similar (BS EN 60300-3-1, 2004).

The allocation of RAMS requirements is dependent on the complexity of these subsystems, based on experience with comparable subsystems. If the requirements are not achieved by the initial design phase, the design process should be repeatedly performed. The allocation is also often made on the basis of considerations, such as complexity, criticality, operational profile and the environmental condition (Ebeling, 2010; MIL-HDBK-388B, 1998).

When the allocation of RAMS requirements is normally conducted in the early design stage, if information available is insufficient, the allocation should be updated continuously through functional analysis. The allocation of RAMS requirements at lower system levels is necessary for the system product definition phase and the aims are set out below (BS EN 60300-1, 2004):

- To confirm the feasibility of RAMS requirements for the entire system,
- To determine verifiable RAMS design requirements at lower levels and,
- To determine clear and feasible RAMS requirements for subsystems and components.

In general, the allocation of RAMS requirements is performed by the following steps:

- Analyse the system;
- Identify areas where design is known and information related to RAMS characteristics available or ready assessed;
- Assign the appropriate weights and;
- Determine their contribution to the top-level RAMS requirement.

MIL-HDBK-388B (1998) provides four techniques for allocation of RAMS requirements as set out below:

- Equal allocation technique;
- ARINIC[12] allocation technique;
- Feasibility of objective technique, and;
- AGREE[13] technique.

It should be noted that the equal allocation technique is an apportionment technique that equally allocates the reliability requirement of the system to all subsystems. It is usually used when there is no information available for the subsystems to design. The ARINIC technique is applied when the failure rate of the subsystems is the only one available. The allocation is conducted by the weight factor that a subsystem contributes to the failure of the system. The feasibility technique is used according to appropriate experience and knowledge of the designers related to the subsystems and these techniques consider the system complexity, environment and operation as well as the failure rate. Finally, the AGREE technique allocates system reliability requirements by the complexity of the subsystem and the contribution of the subsystems causes the failure of the entire system. The complexity can apply the number of components that comprise a subsystem and the contribution can be calculated by the failure rate of the entire system over the failure rate of a subsystem (MIL-HDBK-388B, 1998).

3.4.11 Reliability Growth Assessment

Reliability growth assessment (RGA) is applied for the improvement of reliability performance through the systematic and permanent removal of failure mechanism. The RGA

[12] Aeronautical Radio, Incorporated.
[13] Advisory Group on Reliability of Electronic Equipment

aims to assess reliability performance over time through design changes of the system. The RGA is accomplished through implementation of the test-fix-test-fix cycle for the system prototype. There are many reliability growth models in the literature, but Duane and Power Law models are generally used (Rooney et al., 2001; MIL-HDBK-189C, 2011).

The Duane model is the most frequently used model to analyse reliability growth graphically. The model was originally developed by J.T. Duane in 1964 and it is quick, simple and easy to understand. The Duane model uses a deterministic approach to reliability growth such that the Mean Time Between Failure (MTBF) of the system versus operating time is represented as an approximate straight line when it is plotted on 'log-log paper' (Smith et al., 1980; MIL-HDBK-781A, 1996).

The Power Law model (or AMSAA[14] model) was developed by L.H. Crow in the 1970s. The growth pattern of the power law model is the same as the Duane model, but the Power Law model is statistics-based. The statistical structure of the Power Law model is equivalent to a Non-Homogeneous Poisson Process (NHPP) model with Weibull failure rate function. This has several advantages because the parameters of an NHPP can be estimated on a statistically rigorous basis; confidence intervals can be obtained; and Goodness of Fit Test (GFT) can be applied (Smith et al., 1980; Ebeling, 2010; BS EN 61164, 2004).

3.4.12 RAMS Test Assessment

3.4.12.1 Reliability Test Assessment

BS EN 60300-3-5 (2001) classifies reliability tests as estimation, compliance and comparison tests. The reliability estimation test aims to evaluate the reliability measures for the estimation of warranty costs and reliability prediction. The comparison test is for comparison between

[14] Army Materiel Systems Analysis Activity

the reliability performances of functionally similar two systems in order to determine whether system A has higher reliability than system B, rather than to estimate the reliability performance measures between them.

The compliance test (or demonstration test) is used to identify the compliance with specified parameters. The outcome of the test is determined by either "accepted" (compliant) or "rejected" (non-compliant). The test is based on the principle of statistical hypothesis testing. The reliability demonstration test is important in determining the acceptance of the system reliability design. In general, two reliability demonstration methods can be applied to railway system tests: truncated sequential test and fixed duration test (BS IEC 61124, 2006; MIL-HDBK-781A, 1996).

3.4.12.2 Maintainability Test Assessment

As part of system test performing during the system engineering design, a maintainability test is conducted to verify that maintainability requirements are being met by the system design. BS EN 60300-3-10 (2001) and MIL-HDBK-470A (1997) classify maintainability test as two categories: maintainability qualification test and maintainability demonstration test.

The maintainability qualification test can be conducted to confirm that a prototype meets the customer’s requirements in initial studies and during the development of a prototype. This test is not necessarily required, but it is a very effective method to ascertain that maintainability requirements have been met. The maintainability demonstration test is a test which verifies the developed prototype’s fulfilment of maintainability requirements. The test assessment is based on the theory of statistical hypothesis testing and it is applied after completing the final design (BS IEC 706-3, 2006).

3.5 Summary

This chapter presents the overall concepts, methods and techniques of systems engineering to establish the theoretical engineering background relating to systems RAMS management. The systems, risk and system life cycle based approach for implementation of railway RAMS management is the focal point of this chapter. Therefore, this chapter has discussed the definitions, processes, methods and techniques related to the successful implementation of railway RAMS management.

This chapter has firstly reviewed several definitions of system/systems and systems engineering to establish the engineering concepts for the successful realisation of a system. The management activities of systems engineering have been reviewed in three ways: RAMS characteristics, threats and means, to help the thorough understanding of systems RAMS in the management perspective. However, systems engineering is a relatively new engineering concept that has many difficulties to overcome for the application it to railway systems engineering. Accordingly, it is revealed that more study is required to integrate RAMS management into railway systems engineering.

This chapter defines systems RAMS management in four perspectives based on (1) the risk based RAMS management, (2) the definition of RAMS performance characteristics, (3) the assessment and control of the hazard factors affecting RAMS performance and (4) the provision of the means for the prevention of the threating factors. This chapter has also investigated various RAMS risk assessment methods for the actuate risk assessment and the overcoming of the problems due to insufficient information and data with the definition of risk. Typical assessment techniques to support RAMS management are variously investigated and discussed.

Much literature related to this research topic has been reviewed, but the literature survey will be continued during the entire research period of time in order to improve the developed research models and enhance the necessary theoretical background continuously.

Chapter 4

DEVELOPMENT OF PROCESS BASED RAILWAY RAMS MANAGEMENT SYSTEMS

4.1 Introduction

Railway RAMS can be conducted successfully, not only through the achievement of the technical issues, but also through the establishment of the management issues. Thus, it is a prerequisite for the successful implementation of RAMS management establishing the effective management structure and organisational environment. Railway RAMS management is an engineering discipline that shall be implemented as an integrated part of railway systems engineering. Thus, it shall be consistent with the policy, objectives, principles, criteria, techniques, methods and tools of railway systems engineering management. Accordingly, railway RAMS management shall conduct a systematic approach for railway systems engineering to establish the management structure and organisational environment and to make a quick response to the changes of railway systems engineering. However, railway organisations have not established a coherent management structure and environment in the railway project as an integrated part of railway systems engineering. This chapter focuses a systematic approach on the implementation of RAMS management for railway systems engineering.

This chapter comprises five sections to present a systematic approach of railway RAMS management. Section 4.2 presents the methods to develop a railway RAMS management systems. Section 4.3 deals with railway systems engineering process and its process activities.

Section 4.4 presents risk based RAMS management process. This chapter finally concludes with a brief summary in Section 4.5.

4.2 Development of Railway RAMS Management Systems

4.2.1 Railway RAMS Management

Railway is a complex engineering system that works together with various typical engineering disciplines as stated in Chapter 1. Therefore, railway industry has considered or addressed the introduction of systems engineering in the railway projects as an interdisciplinary means of the various engineering disciplines to develop the steadfast conceptual design criteria and take a role of a bridge between railway systems engineering and the traditional engineering disciplines[15]. On the other hand, the objective of railway is to perform a defined railway traffic service safely within a scheduled time and limited budget. For the achievement of the railway service objective, railway industry has also addressed the integration of RAMS management into railway systems engineering as a comprehensive engineering management discipline for the achievement of safety and time dependence performance. However, many railway organisations have not implemented the RAMS management successfully because of the lack of systematic approach for systems engineering. Therefore, it becomes a great significant challenge to integrate RAMS management into railway systems engineering (BS EN 50126-1, 1999).

Railway systems engineering has been focused on the successful realisation of a system as a whole for all function and performance requirements. The system performance is defined through the assessment of railway risks to reduce or eliminate all potential threats to the rail traffic service as minimum as possible. Accordingly, the assessment of railway risks is a

[15] Mechanical, Electrical, Electronics, Civil and Software Engineering

major focus of railway systems engineering and the assessment results are controlled by RAMS management as shown in Figure 4.1. Many inherent risks which have been identified and experienced from the railway operational contexts, such as operation, system, maintenance and the maintenance support conditions, and the challenges which have been posed from many railway engineering projects shall be continuously managed from the system concept design stage to the detailed design phase. This is because the railway risks have a great potential to cause injury and/or loss of life to the staff or passengers, environmental degradation, damage to the railway property or freight and adverse impact for railway service. Therefore, railway RAMS management shall require a systematic approach for railway RAMS risks and the risk assessment is a core part of the RAMS management process (An et al., 2007; Umar, 2010).

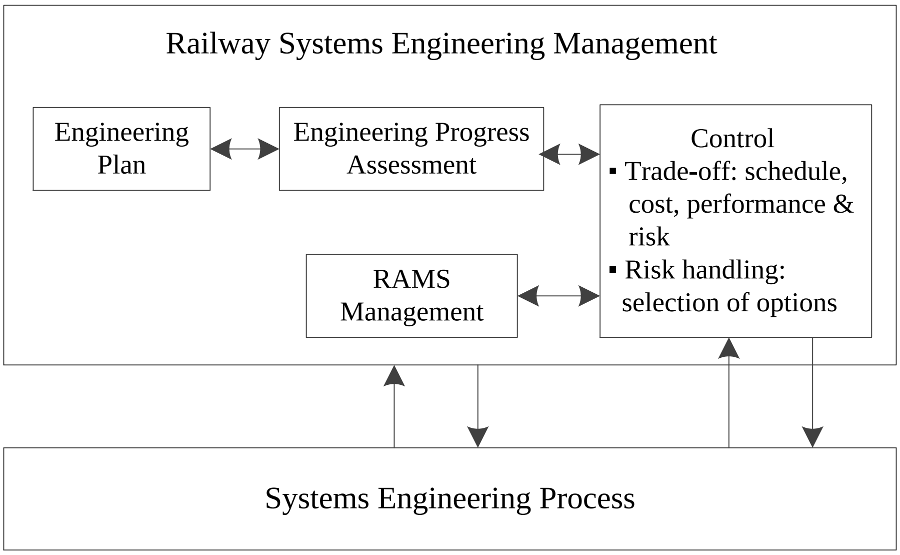

Railway Systems Engineering Management
Engineering Plan
Engineering Progress Assessment
Control
▪ Trade-off: schedule, cost, performance & risk
▪ Risk handling: selection of options
RAMS Management
Systems Engineering Process

Figure 4.1 Concept of Risk Based Railway RAMS Management

4.2.2 Railway Systems Engineering Management

As described in Figure 4.1, RAMS management shall be implemented as an integrated part of railway systems engineering. The railway systems engineering conducts an interdisciplinary approach as a technical and management means to facilitate the design and development and to success railway project. Thus, railway systems engineering is essential to integrate RAMS characteristics needed in the operational contexts into system product design property. The railway systems engineering shall be required, not only in the technical aspects, but also in the management aspects. Railway systems engineering management shall establish a set of the management structure and organisational environment as a system and it also includes the systems engineering management process to solve the problems and challenges effectively. The railway systems engineering management generally conducts the following three activities (Blanchard, 2012):

- Implementing railway systems engineering process;
- Controlling the baselines of railway system design and development phases and,
- Integrating railway system life cycle functions.

The baseline control of the design and development phases, including the trade-off of risk, cost and operational effectiveness and the section of risk handling options, takes a significant role in the railway systems engineering management. The design of a railway system is progressively implemented through several design phases, such as system concept phase, system definition phase, and subsystem and component design phase. The system concept phase is to establish the concepts of the system to design; it is often called the feasibility study phase. The system definition phase provides a description for all system requirements related to the system functions and performances. The subsystem design phase is to establish a description of the system's functional architecture as a preliminary design stage. The component design phase produces a set of the physical design architecture and their performance characteristics as a detailed design phase. Each design phase comprises the baselines in the operational, functional and physical product aspect. The baselines are important control points of the railway systems engineering management (Daup, 2001).

The railway systems engineering management is implemented through the use of systems engineering process to produce the effective technical design criteria for the needs and expectations that are required for a railway system. The system engineering process can be applied to all stages of the systems engineering design; its major functions can be described below (Blanchard, 2012).

The systems engineering process takes the following three roles:

- Transforming customer's system requirements into a set of design solutions and their acceptance performance criteria, and process descriptions;
- Producing all information required for the decision making of system engineering management, and;
- Providing input for the implementation of the next phase in each system design phase.

Another activity of the railway systems engineering management is to integrate all functions which may be required or occur throughout the life system cycle into the systems engineering process in order to effectively resolve all possible problems that may occur during the system life cycle and to ensure the feasibility of the railway system in the operation and maintenance phase. RAMS management shall be consistent with the three management activities.

In conclusion, the three roles of railway engineering management: the baseline control of design and development phase, the implementation of systems engineering process and the integration of system life cycle functions, are the major focus of railway RAMS management functions; they become a fundamental basis of the railway RAMS management activities.

4.2.3 Development of Railway RAMS Management Systems

4.2.3.1 Systems Approach to Railway RAMS Management

As stated above, RAMS management shall be implemented as an integrated part of railway systems engineering management; hence, it is subjected to the systems approach for the systems engineering management as shown in Figure 4.2. The systems approach means the study of an organisation's management structure and environment as a system in the whole aspect so that the objective of organisation can be achieved as effectively as possible. In the same way, it is also necessary to consider the objectives of individual management activities very carefully. The systems approach requires that the individual management activities shall be brought together in the form of the organisation’s objective as a whole. Figure 4.2 describes a systems approach model of RAMS management for railway engineering management. Therefore, RAMS management requires the systems approach to be integrated into systems engineering management as shown in Figure 4.2 (BS ISO 9000, 2005).

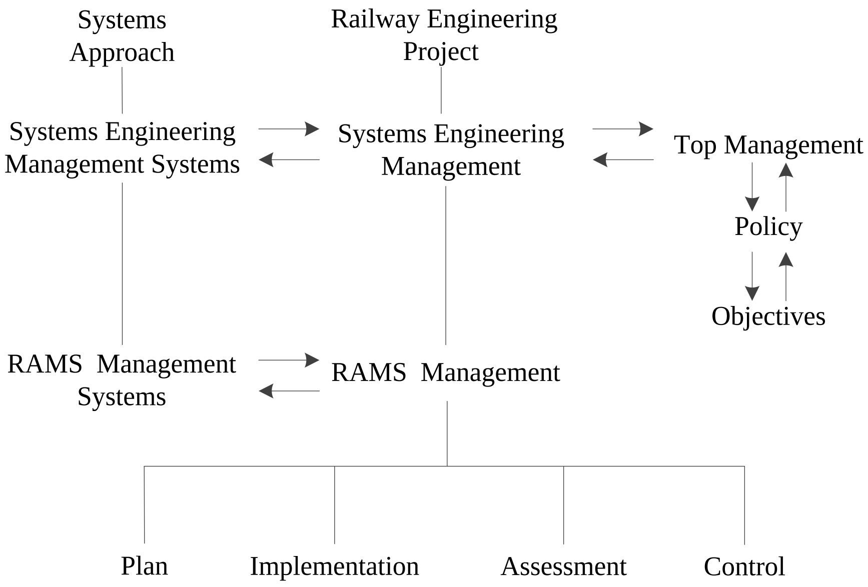


Figure 4.2 Systems Approach to Railway RAMS Management

4.2.3.2 Development of Railway RAMS Management Systems

It is essential to establish RAMS management at the early concept phase of system design as well as develop the RAMS management systems. However, the development principles and methods of the RAMS management systems are not yet established and have not been provided from the railway industry. Figure 4.3 shows a proposed framework that develops a railway RAMS management systems, which is based on the definition of the systems approach reviewed in Chapter 3.

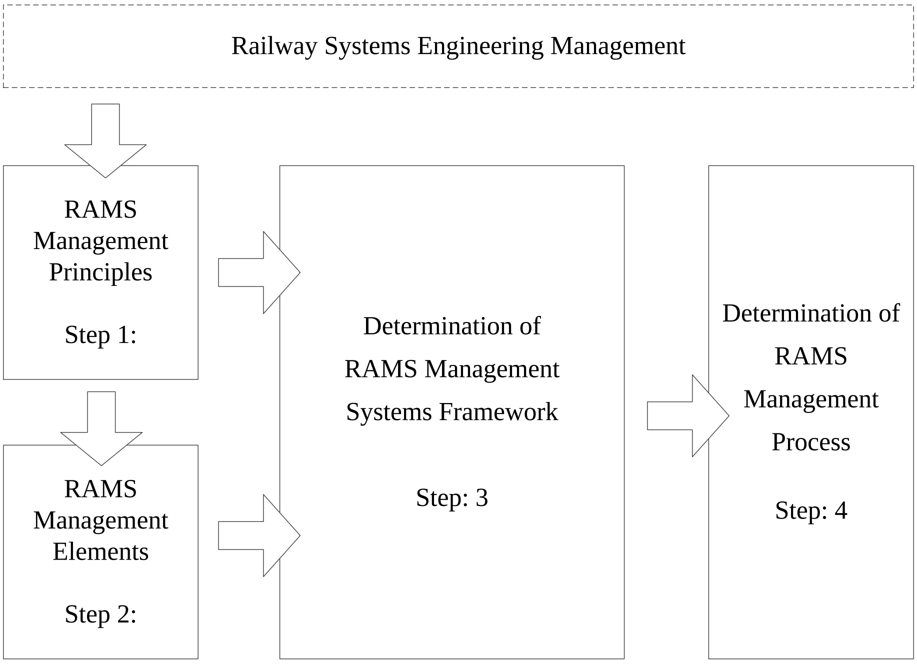

Railway Systems Engineering Management
RAMS Management Principles
Step 1:
RAMS Management Elements
Step 2:
Determination of RAMS Management Systems Framework
Step: 3
Determination of RAMS Management Process
Step: 4

Figure 4.3 Development of Railway RAMS Management Systems

RAMS management systems shall be developed, based on the thorough understanding of the overall systems engineering project. The procedure for development of a RAMS management systems consists of the following four steps as shown in Figure 4.3: (1) the establishment of the fundamental principles of RAMS management, (2) the determination of the major elements of RAMS management, (3) the determination of RAMS management systems framework and (4) the development of the technical RAMS management process.

Step 1: Definition of RAMS Management Principles

Defining the principles of RAMS management is a prerequisite to successfully lead RAMS organisation to improve system's RAMS performance. In general, RAMS management principles shall provide a basic proposition that serves the functional behaviours of the RAMS organisation as a system (Oxford, 2012). Therefore, the following seven items suggest as the principles of railway RAMS management, referred from BS ISO 9000 (2005) and BS EN 60300-1 (2003):

- To focus on the customer's requirements, to achieve the customer's requirements successfully and even strive to exceed the requirements;
- To establish leadership, which aims to establish the RAMS management policy and continuously improve the environment and performance of the RAMS organisation;
- To involve the customers to RAMS management, which aims to achieve the customer requirement and satisfy them effectively;
- To apply systems approach to RAMS management, to increase the synergy of management by the interaction of the interrelated processes and system elements;
- To apply process approach to all system elements of RAMS management systems, to solve the managerial and technical issues more efficiently,
- To continuously improve the performance of RAMS organisation and system products, for the steady and incremental performance improvement of overall organisation and system products and;
- To use statistical techniques to RAMS assessment, to support the precise decision making of RAMS management.

Step 2: Determination of RAMS Management Elements

The second step is to determine the appropriate management elements in order to establish the RAMS management policy and strategy, to coordinate the management functions, and to direct and control the management activities effectively. Accordingly, the RAMS management elements should consider including the following seven activities, referred from BS ISO 9001 (2008) and BS EN 60300-1 (2003):

- To determine RAMS management activities needed;
- To establish RAMS management policy and objectives;
- To determine appropriate system life cycle phases;
- To establish the time phased activities of RAMS management in the systems engineering process stages;
- To determine the acceptance criteria and methods for RAMS requirements;
- To provide necessary resources and information, and;
- To monitor and review the results of RAMS management activities.

Step 3: Integration of RAMS Management Elements as a System

RAMS management elements shall comprise a framework as a system to determine the sequence and interaction of the management elements. Figure 4.4 shows the concept of integrating RAMS management elements based on the principle of PDCA[16] cycle (BS ISO 9000, 2005). In the PDCA cycle, the ‘Plan’ includes the objectives and processes necessary to meet the customer requirements and the organisation’s policies. The ‘Do’ includes directing the implementation of the processes and objectives. The ‘Check’ includes monitoring and measuring the results of all of process activities, and assessing the process results against the

[16] Plan-Do-Check-Act

policy, objectives and requirements, as well as reporting all of the achieved results. Finally, the 'Act' includes conducting corrective or preventive actions to continually improve process performance (BS ISO 9001, 2008).

Figure 4.4 describes the concept for developing a framework of RAMS management systems, which integrates the management and technical elements into the framework of a PDCA cycle. A proposed framework based on Figure 4.4 will be described in the next section.

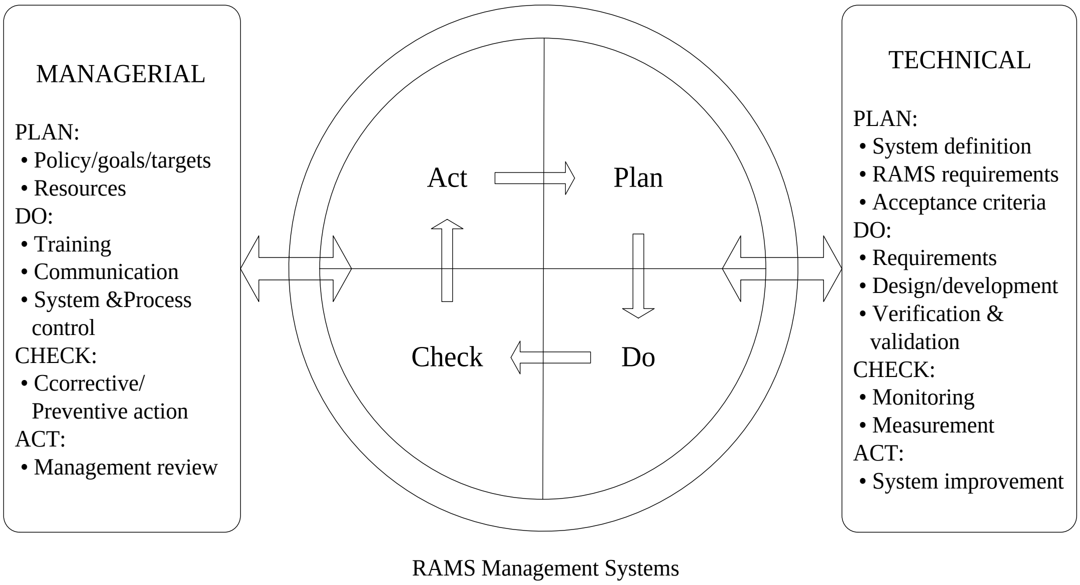


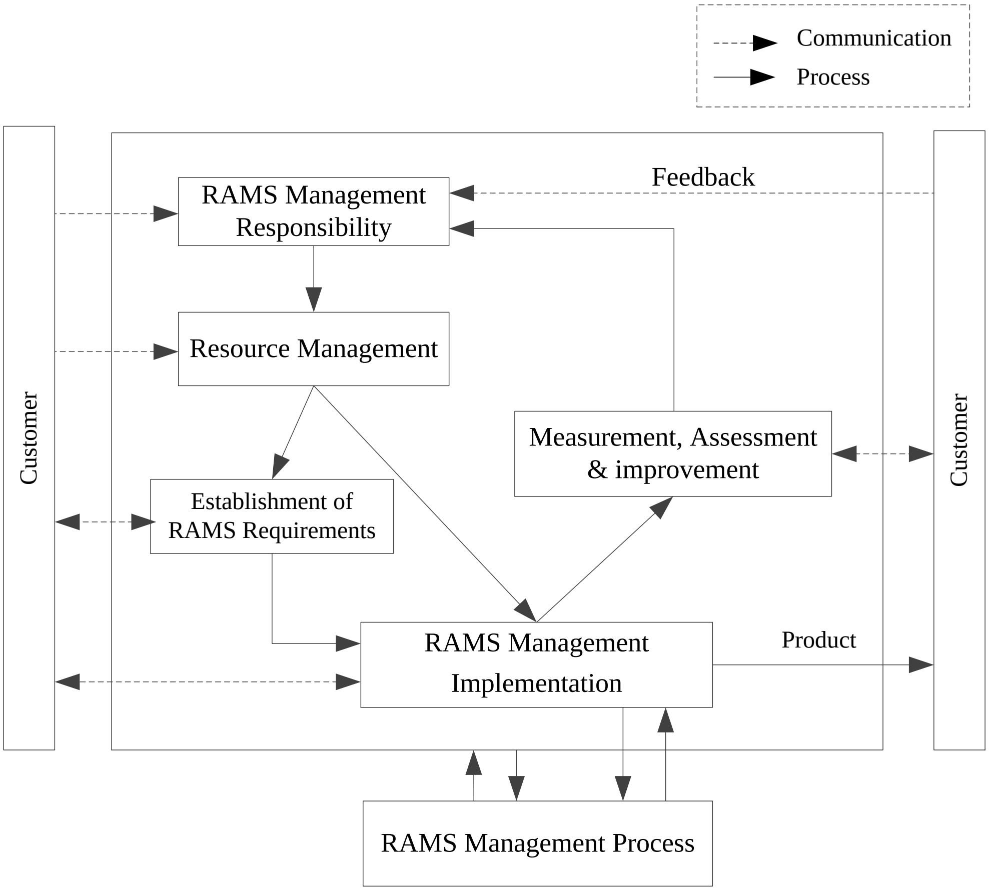
Figure 4.4 Concept of Railway RAMS Management Systems

Step 4: Development of RAMS Management Process

RAMS management shall be focused on the technical management process to achieve the objectives of the RAMS management effectively. The technical management process includes the technical management elements to define, analyse, evaluate and control RAMS characteristics as described in Figure 4.4; it shall be implemented in the systems engineering process. Therefore, the establishment of the systems engineering process is essential to provide the basis to the process activities of RAMS management. Accordingly, the process and its activities of the systems engineering will be presented with several models in Section 4.3 and the RAMS management process will be presented in Section 4.4 of this chapter.

4.2.3.3 A Proposed Framework of Railway RAMS Management Systems

Until now, the method has been discussed in which a railway RAMS management systems is developed to direct the RAMS management policy, control the management functions and coordinate the management activities. Figure 4.5 describes a proposed process based RAMS management systems model that is comprised of six management elements. The management activities of six system elements and their interactions are established on the basis of the principles of PDCA cycle, process and systems.



Communication
Process
Customer
RAMS Management Responsibility
Feedback
Resource Management
Measurement, Assessment & improvement
Customer
Establishment of RAMS Requirements
RAMS Management Implementation
Product
RAMS Management Process

Figure 4.5 Proposed Process based Railway RAMS Management Systems Model

(1) Determination of RAMS Management Responsibility

RAMS organisation should determine the overall management responsibility for the strategic policy and objectives of RAMS management as shown in Figure 4.2. The management responsibility contains the requirements for top management activities. The top management means a leader of an organisation to achieve the organisational objective. The management responsibility can generally include the following six elements for RAMS management: (1) commitment and function, (2) strategy, (3) policy, (4) planning, (5) responsibility, authority and communication and (6) management review (BS EN 60300-2, 2004).

(2) Establishment of Resource Management

As mentioned above, RAMS management takes a role of optimally allocating the limited resources to achieve the operational objectives successfully. Therefore, adequate resource management is a key factor for the successful achievement of RAMS management, and for the continuous implementation and maintenance of RAMS management systems. Therefore, the resource management is specially included as an individual RAMS management element that is separated from RAMS management responsibility. The major role of the resource management includes the following three elements: (1) organisation's personnel and expertise, (2) financial resources and (3) information and data resources including RAMS knowledge base. The resource of information and data is the key factor to meet the RAMS performance requirements (BS EN 60300-1, 2004).

(3) Establishment of customer RAMS Requirements

RAMS organisation should support the establishment of customer RAMS requirements in order to facilitate the RAMS specification process. In general, a customer has the weak point in the accurate understanding of systems, risk and system life cycle management concepts for the recent systems engineering and in the numeral expression of the RAMS characteristics of all functional requirements. Therefore, the supplier and customer should establish the RAMS requirements together through the analysis of resources, system's needs and expectations, which are provided by the customer.

(4) Implementation of RAMS Management

RAMS organisation should implement the planned management activities and achieve RAMS requirements, which are implemented through technical RAMS management process as shown in Figure 4.5. To implement the RAMS management, an appropriate schedule, policy and strategy are included in the RAMS management process. However, the RAMS management process has to be implemented into the systems engineering process. RAMS management process will be in detail dealt with in Section 4.4 (BS ISO/DIS 31000, 2008).

(5) Measurement, Assessment and Improvement of RAMS Management Systems

RAMS organisation should plan and implement a process that can monitor, measure, assess and improve the effectiveness of RAMS management systems. The RAMS organisation should continually improve the effectiveness of the RAMS management systems through the above process activities. The results of measurement and assessment are significant foundations to continuously improve the RAMS management systems (BS EN 60300-2, 2004).

4.2.3.4 Integration of RAMS Management Systems into Railway Systems Engineering

Figure 4.6 describes a proposed model for integrating RAMS management into railway systems engineering. As shown in Figure 4.6, RAMS management is implemented as an integrated part of railway systems engineering management. The RAMS management activities are dependent on the results of the systems engineering process. Therefore, the establishment of the systems engineering process activity is essential to implement RAMS management process. Section 4.3 will present the detailed activities of systems engineering process to establish the functions and activities of RAMS management.

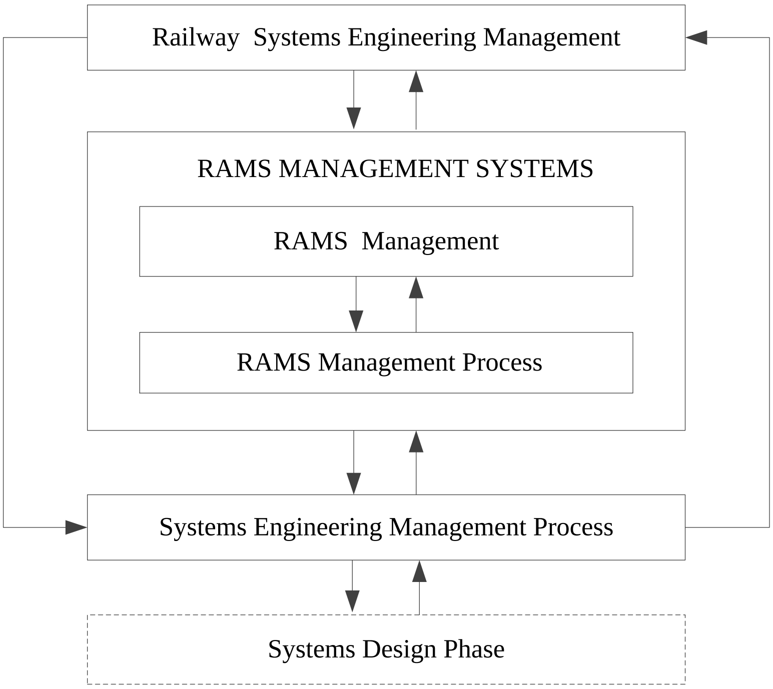


Figure 4.6 Integration Model of RAMS Management into Railway Systems Engineering

4.3 Establishment of Railway Systems Engineering Process

RAMS management is performed through railway systems engineering process. Therefore, it is necessary to establish the railway systems engineering process and its process activities. BS EN 50126-1 (1999) provides the system life cycle based railway systems engineering process with the general management activities, but it is comprised of highly simplified sequential phases from concept to decommissioning, as shown in Figure 4.7 and Table 4.1.

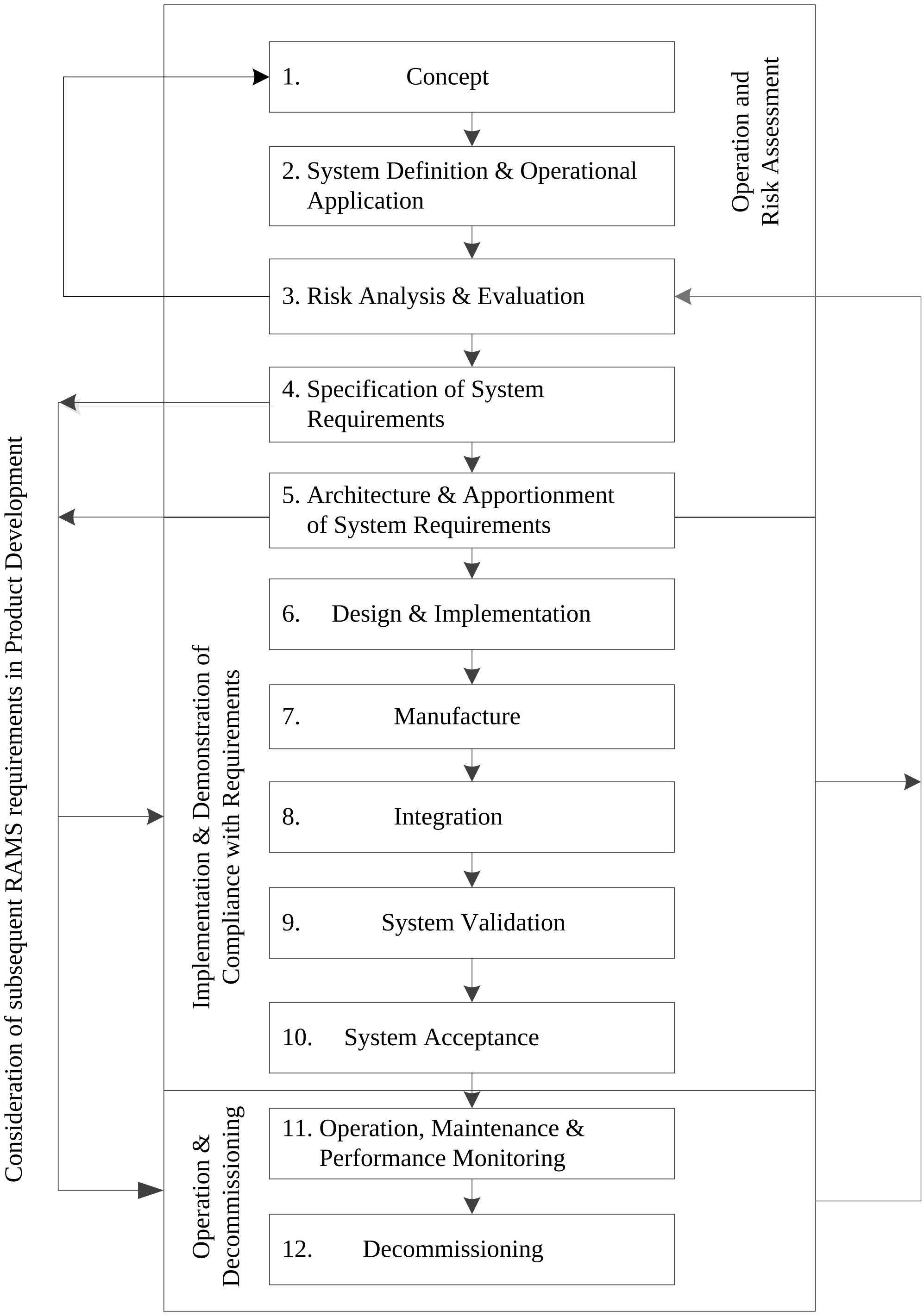

1. Concept
2. System Definition & Operational Application
3. Risk Analysis & Evaluation
4. Specification of System Requirements
5. Architecture & Apportionment of System Requirements
6. Design & Implementation
7. Manufacture
8. Integration
9. System Validation
10. System Acceptance
11. Operation, Maintenance & Performance Monitoring
12. Decommissioning
Operation and Risk Assessment
Implementation & Demonstration of Compliance with Requirements
Operation & Decommissioning
Consideration of subsequent RAMS requirements in Product Development

Figure 4.7 Typical Railway Systems Engineering Process

Table 4.1 System Life Cycle Management Tasks

Life-cycle Phase	General Management Tasks
1. Concept	- Establish railway project. - Undertake feasibility studies. - Establish systems management.
2. System definition & operational applications	- Establish mission profile. - Identify operational applications.
3. Risk analysis & evaluation	- Undertake risk analysis and evaluation.
4. Specification of system requirements	- Undertake system requirements analysis. - Specify system, operational contexts and environment. - Establish system verification plan.
5. Architecture & apportionment of system requirement	- Apportion systems requirements. - Specify subsystem & component requirements**.** - Define subsystem & component acceptance criteria.
6. Design & implementation	- Perform design & development. - Perform design analysis & test. - Perform design verification.
7. Manufacture	- Perform production plan. - Establish training.
8. Integration	- Assembly system. - Install system.
9. System validation	- Commission. - Perform probationary period of operation.
10. System acceptance	- Undertake acceptance procedure. - Compile evidence for acceptance.
11. Operation, maintenance & performance	- Perform operation & maintenance. - Collect operational performance statistics. - Acquire, analyse & evaluate data.
12. Decommissioning	- Plan decommissioning and disposal.

However, the sequential phase may not be effective in implementing the management activities of railway systems engineering. In practice, the phases are overlapped and repeated as a process that integrates the possible system life cycle functions to find out the solutions for the best, optimal and balanced design, and to ensure the feasibility in the operational phase. Thus, the processes of Figure 3.4 and 4.7 can be modified as a process based model as depicted in Figure 4.8.

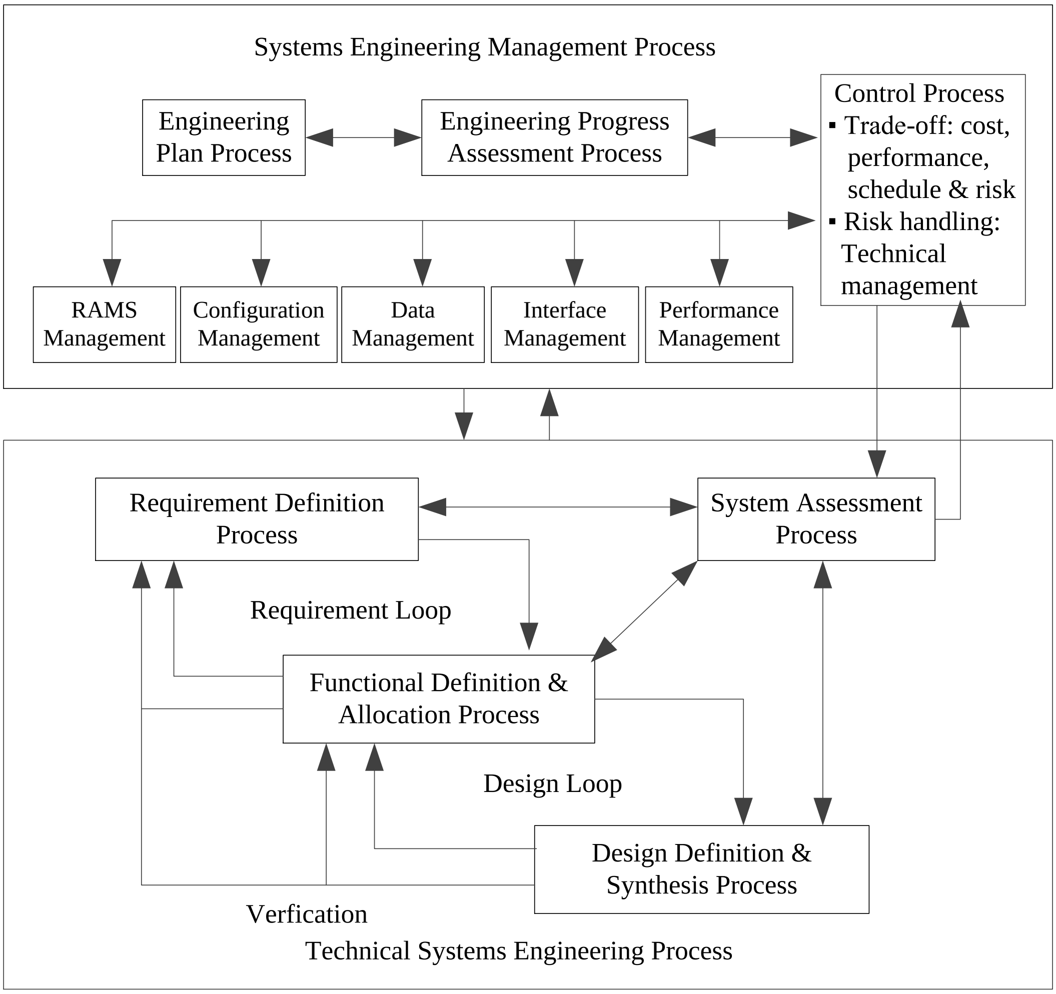

Systems Engineering Management Process
Engineering Plan Process
Engineering Progress Assessment Process
Control Process
▪ Trade-off: cost, performance, schedule & risk
▪ Risk handling: Technical management
RAMS Management
Configuration Management
Data Management
Interface Management
Performance Management
Requirement Definition Process
System Assessment Process
Requirement Loop
Functional Definition & Allocation Process
Design Loop
Design Definition & Synthesis Process
Verfication
Technical Systems Engineering Process

Figure 4.8 Modified Process Based Railway Systems Engineering Model

The proposed systems engineering model is divided into the technical systems engineering process that implements and assesses the technical system management, and the systems engineering management process to trade off and control the results of the technical process activities as shown in Figure 4.8. The management process is a process that trades off, controls and selects the assessment results of the technical process activities for the planned management. The technical process is a process that is conducted to find out the technical design solutions and acceptance performance criteria through the assessment of requirements, functional behaviours and design alternatives. The technical process consists of three baseline phases to conduct the systems engineering management process activities.

The requirement definition phase establishes the requirement baseline. The functional definition and allocation phase establishes the functional architecture baseline. The design definition and synthesis phase determines the design architecture baseline. These baseline phases are the significant decision-making points of the systems engineering management.

As seen in Figure 4.8, the technical systems engineering process has two process loops to represent the iterated process activities: requirement and design loop. The requirement loop aims to define the functional and performance requirements. The design loop aims to establish the design architecture and performance characteristics. Each loop activity also establishes the functional architecture. The results produced from the engineering process phase are verified through inspection, analysis, test or demonstration.

4.3.1 Requirement Definition Phase

This phase is a process which assesses customer’s requirements to define the level or quantitative value of system requirements needed in the system design. Figure 4.9 describes the major four process activities of this phase: operational scenarios definition, measures of effectiveness definition, functional requirements definition and performance requirements definition. Figure 4.10 provides the expanded framework that includes the major activities and their assessment elements.

This phase begins with identifying the customer’s requirements and the internal and external constraints related to the engineering implementation. The measures of effectiveness and the operational scenarios are defined through the assessment of system boundaries and interfaces, operational environments and the life cycle process. The functional and performance requirements are defined with assessment of modes of operation, technical performance, human factors and functional behaviour analysis for the operational scenarios as Figure 4.10.

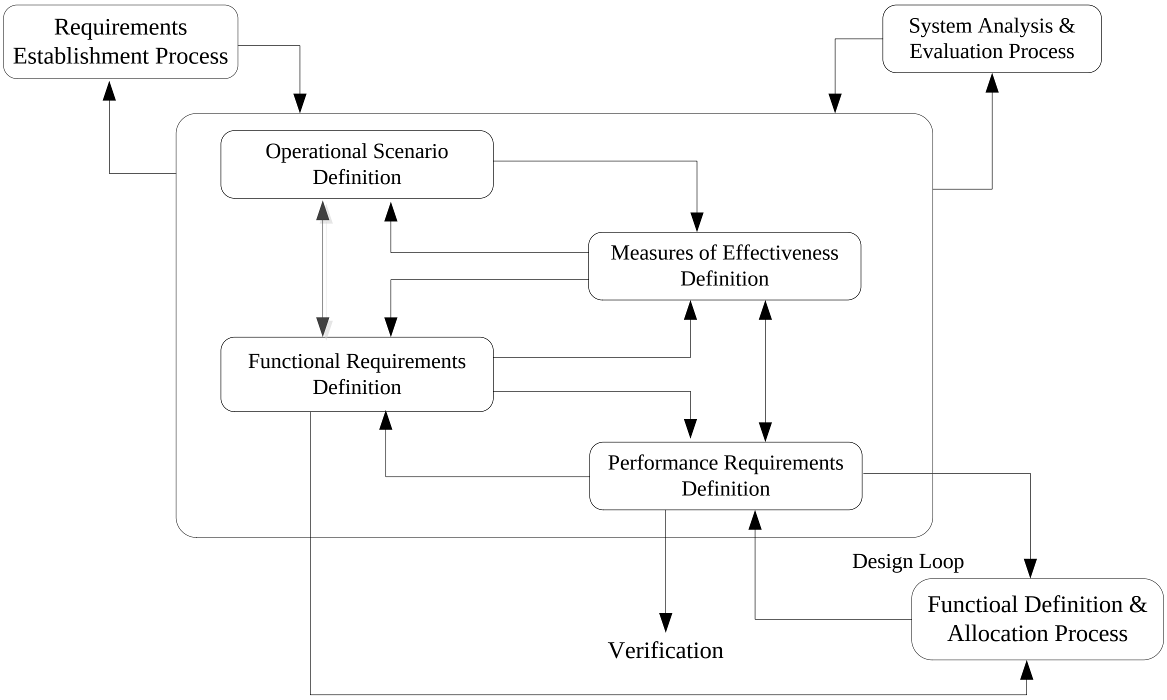

Requirements Establishment Process
System Analysis & Evaluation Process
Operational Scenario Definition
Measures of Effectiveness Definition
Functional Requirements Definition
Performance Requirements Definition
Design Loop
Functioal Definition & Allocation Process
Verification

Figure 4.9 Requirement Definition Process

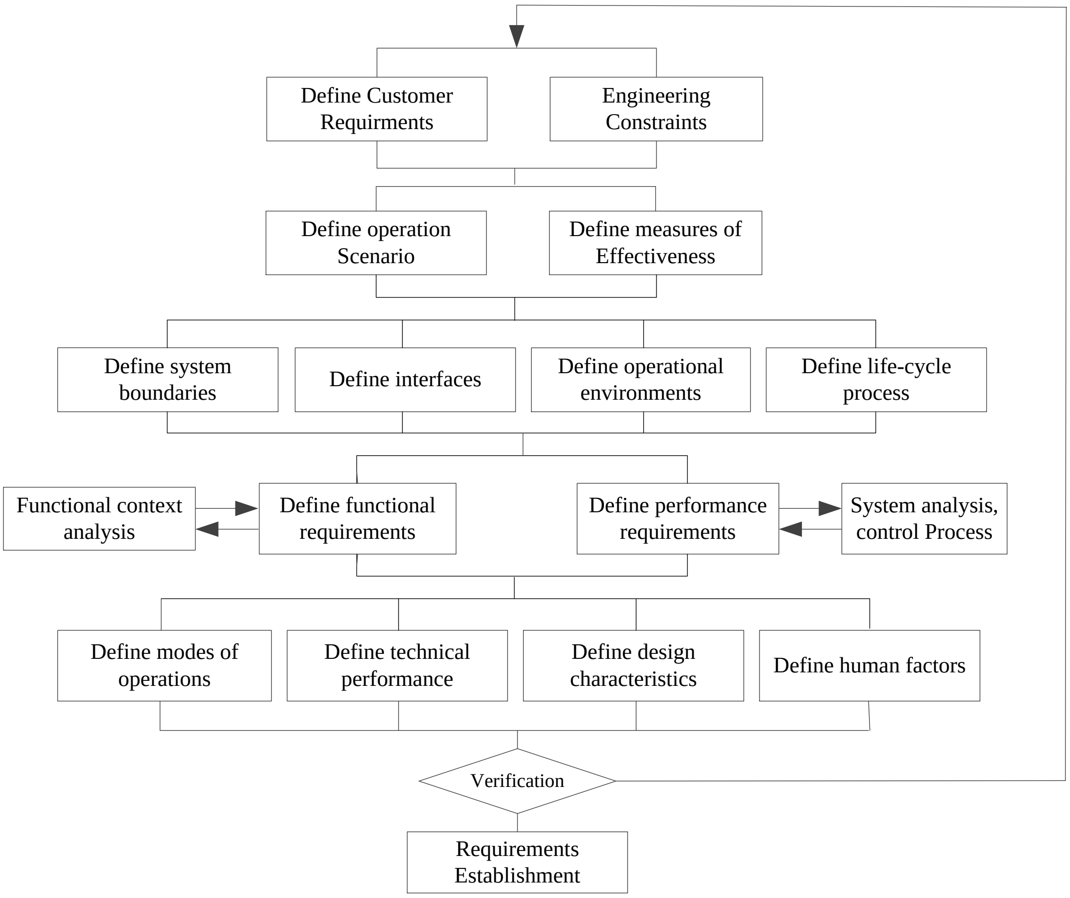

Define Customer Requirments
Engineering Constraints
Define operation Scenario
Define measures of Effectiveness
Define system boundaries
Define interfaces
Define operational environments
Define life-cycle process
Functional context analysis
Define functional requirements
Define performance requirements
System analysis, control Process
Define modes of operations
Define technical performance
Define design characteristics
Define human factors
Verification
Requirements Establishment

Figure 4.10 Requirement Definition Process Activities

4.3.2 Functional Definition and Allocation Phase

This phase is a process that defines the functional architecture through allocation method. The functional behaviours and their interfaces analysis and the performance requirement allocation are the basis activities of this process phase. The sub-function definition and the performance allocation are established by the analysis of sub-function states and modes, as shown in Figure 4.11. Figure 4.12 describes the more detailed activities of this process.

This phase commences with the analysis of the functional behaviours and their interfaces for the operational scenarios and the allocation of system performance requirements, which form the basis of the definition of sub-function states and modes and which are determined through the analysis of functional timeline, data and control flow, and functional failure modes and effects. The failure modes and their effects are analysed to determine safety functions and their monitoring functions as shown in Figure 4.12.

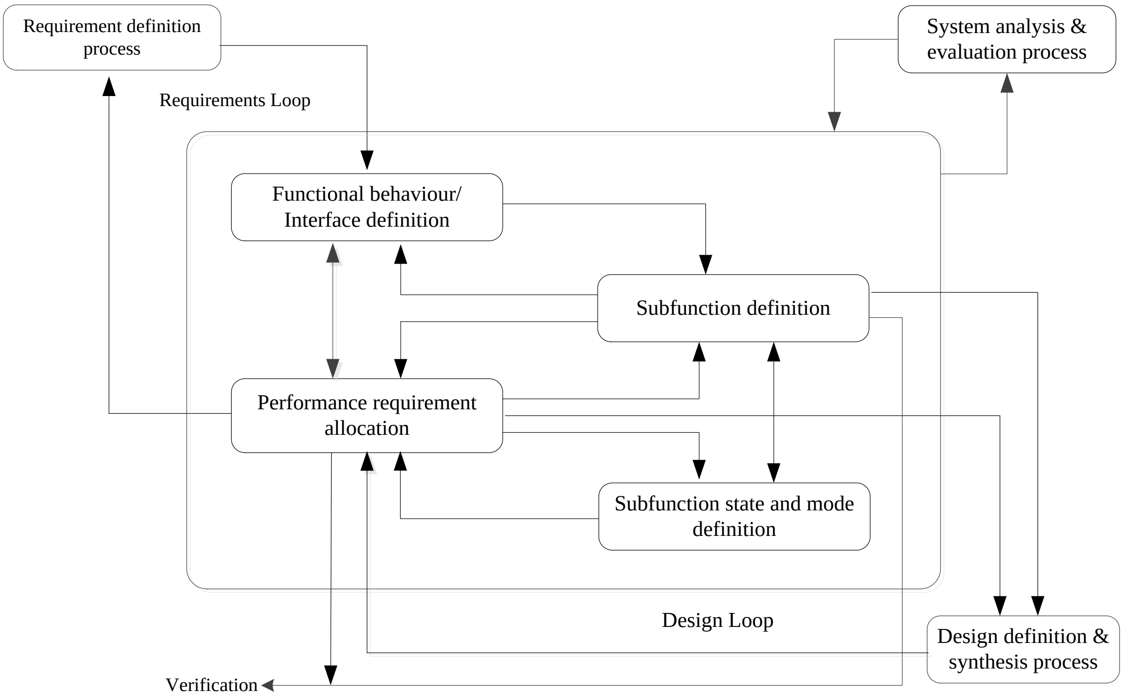

Requirement definition process
System analysis & evaluation process
Requirements Loop
Functional behaviour/ Interface definition
Subfunction definition
Performance requirement allocation
Subfunction state and mode definition
Design Loop
Design definition & synthesis process
Verification

Figure 4.11 Functional Definition & Allocation Process

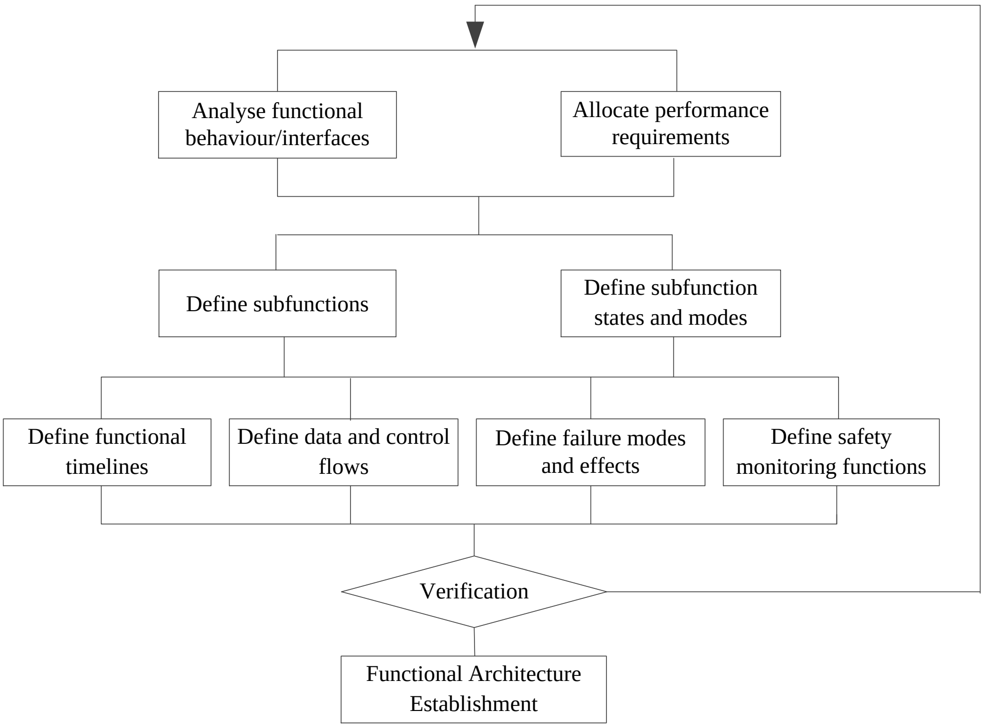

Analyse functional behaviour/interfaces
Allocate performance requirements
Define subfunctions
Define subfunction states and modes
Define functional timelines
Define data and control flows
Define failure modes and effects
Define safety monitoring functions
Verification
Functional Architecture Establishment

Figure 4.12 Function Definition and Allocation Process Activities

4.3.3 Design Definition and Synthesis Phase

This phase is a process that defines physical designs (components), their performance characteristics and the physical interfaces which comprise a subsystem. The establishment of the design solution alternatives and the assessment of the model or prototype are the major roles of this phase as shown in Figure 4.13. Figure 4.14 provides the expanded framework that includes detailed process activities based on Figure 4.13.

The establishment of subsystems and their design solution alternatives are conducted through the assessment of safety hazards, life cycle quality factors and technical requirements, as depicted in Figure 4.14. The definition of design and their performance characteristics are established by the development of models or/and prototypes, and then the assessment of failure modes and effects, testability and design capacity of the developed models and prototypes as shown in Figure 4.14.

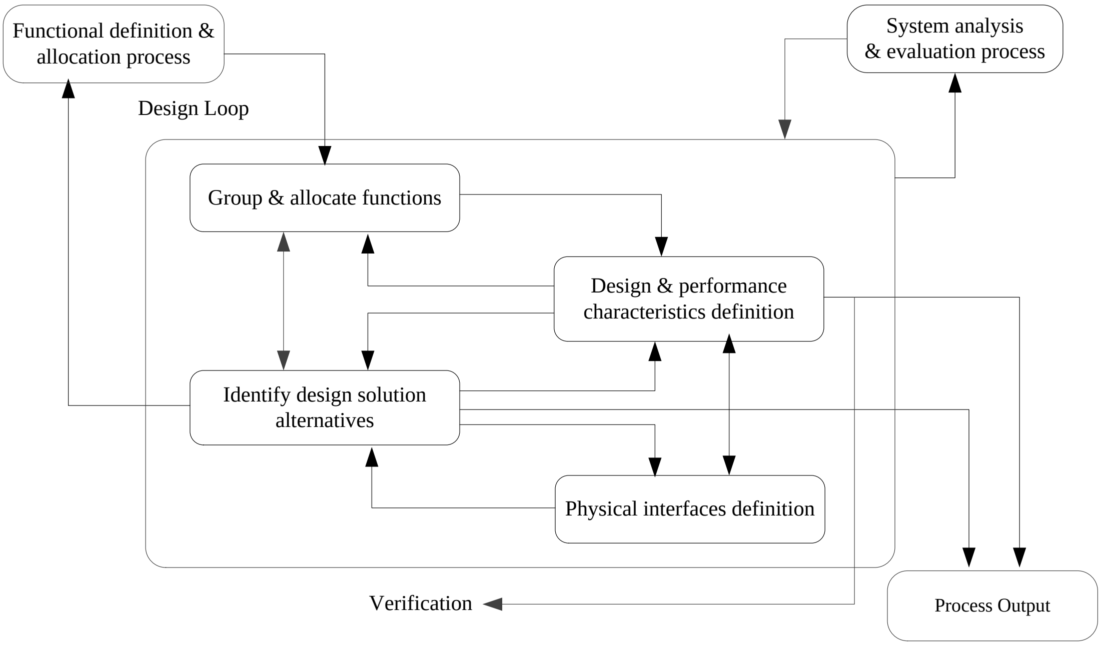

Functional definition & allocation process
System analysis & evaluation process
Design Loop
Group & allocate functions
Design & performance characteristics definition
Identify design solution alternatives
Physical interfaces definition
Verification
Process Output

Figure 4.13 Design Definition & Synthesis Process

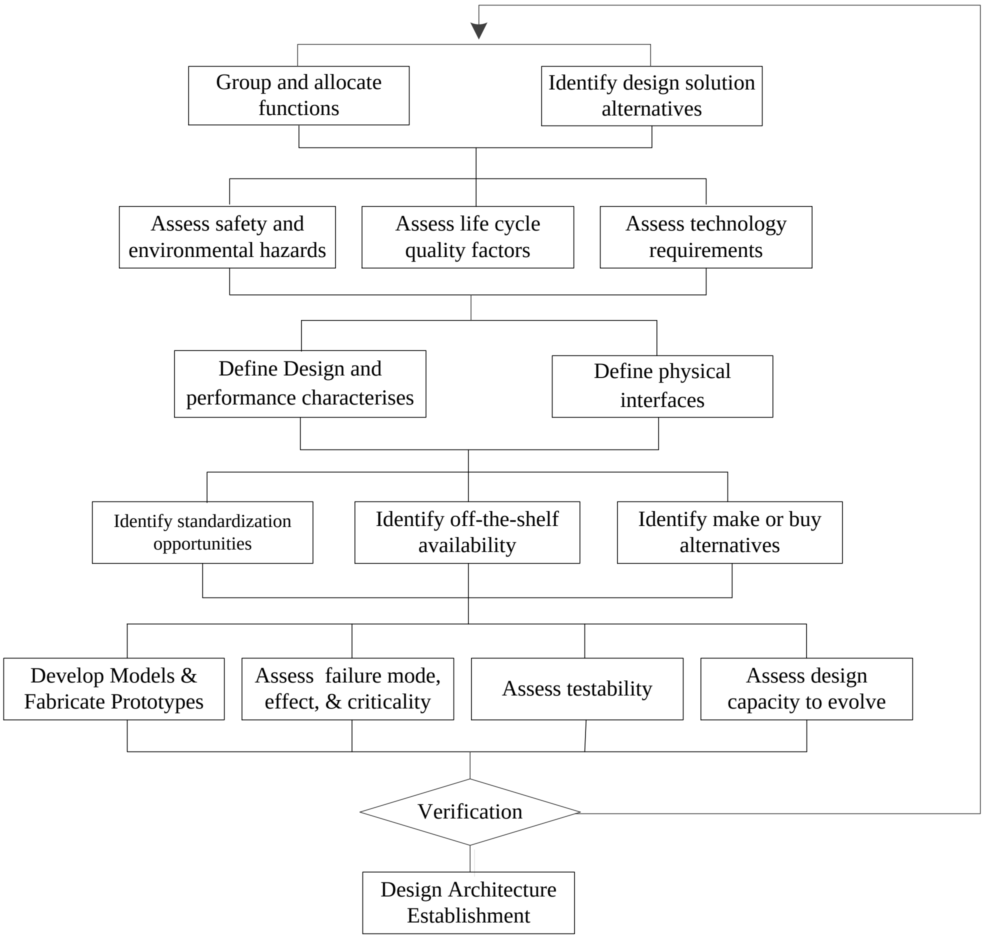
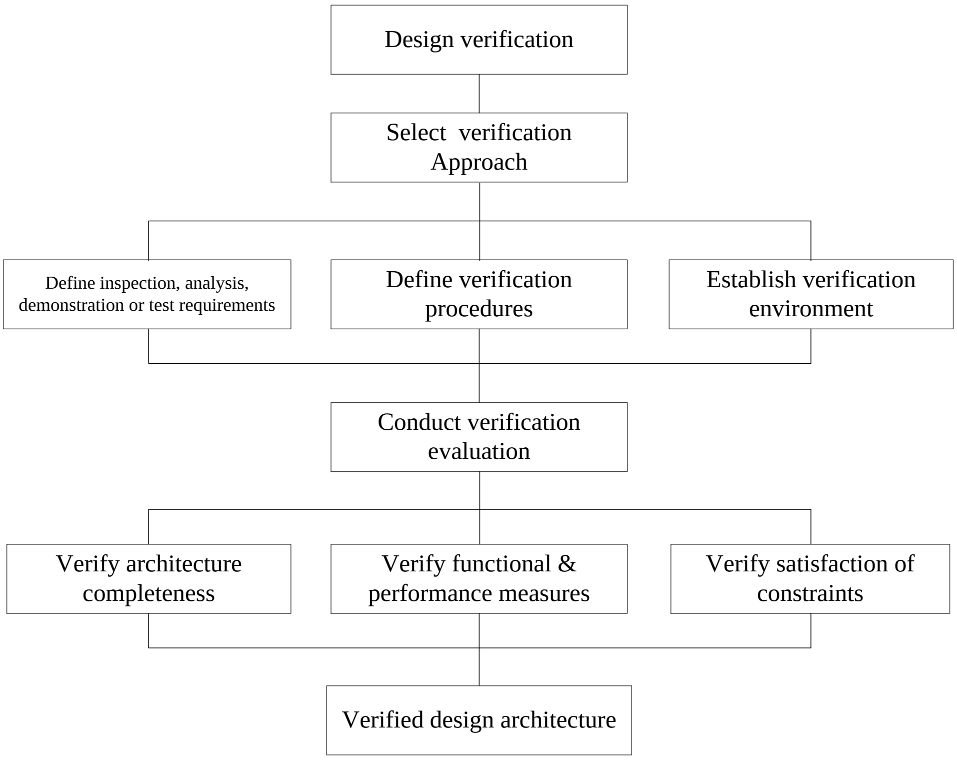

Group and allocate functions
Identify design solution alternatives
Assess safety and environmental hazards
Assess life cycle quality factors
Assess technology requirements
Define Design and performance characterises
Define physical interfaces
Identify standardization opportunities
Identify off-the-shelf availability
Identify make or buy alternatives
Develop Models & Fabricate Prototypes
Assess failure mode, effect, & criticality
Assess testability
Assess design capacity to evolve
Verification
Design Architecture Establishment

Figure 4.14 Design Definition & Synthesis Process Activities

4.3.3.1 Design Verification

Verification is commonly conducted in all engineering process phases. However, the design verification is the most important part in the systems engineering process phase because the verification principle includes the methods using in the other process phases. Figure 4.15 depicts the verification method that is applied in the design phase, which confirms that the design definition and synthesis process has achieved the design architecture that satisfies the system requirements. The objectives of this process include the confirmation of the established acceptance criteria to conduct the verification of the design architecture, functional and performance measures and design constraints from the lowest level to the entire system level. The design verification is performed by one method among inspection, analysis, demonstration or testing as shown in Figure 4.15.


Design verification
Select verification Approach
Define inspection, analysis, demonstration or test requirements
Define verification procedures
Establish verification environment
Conduct verification evaluation
Verify architecture completeness
Verify functional & performance measures
Verify satisfaction of constraints
Verified design architecture

4.15 Design Verification Procedures

4.3.4 Systems Control Phase

This phase conducts the trade-off and technical managements for the assessment results of all systems engineering process phases. As shown in Figure 4.16, there are three process activities: (1) controlling the assessment results of the systems engineering process, (2) conducting the trade-off for the assessed process results to select risk handling options and (3) implementing the technical management for the selected risk handling options. The detailed tasks of this process are described in Figure 4.17.

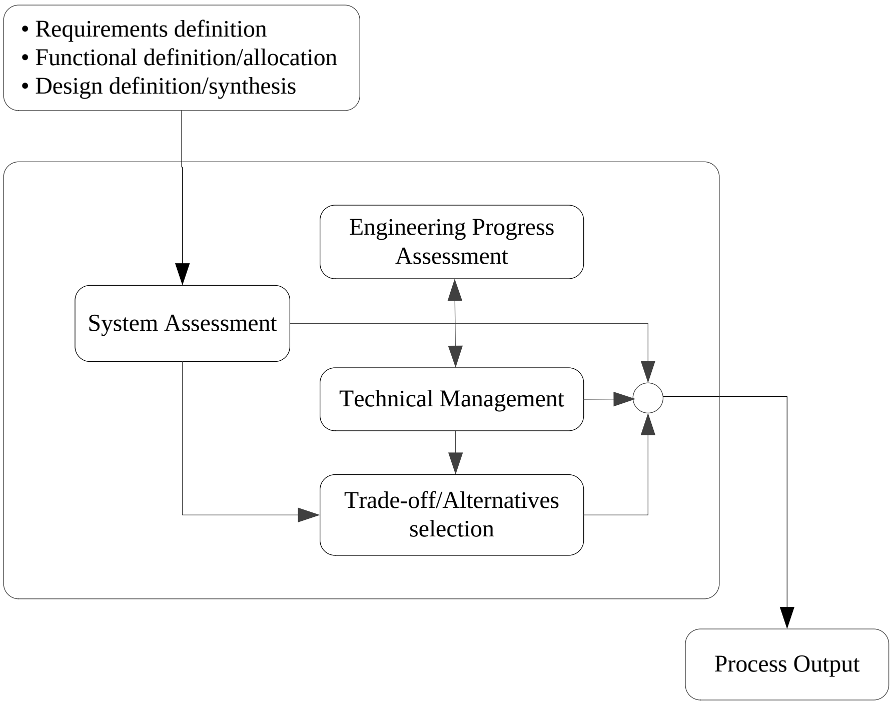

• Requirements definition
• Functional definition/allocation
• Design definition/synthesis
Engineering Progress Assessment
System Assessment
Technical Management
Trade-off/Alternatives selection
Process Output

Figure 4.16 Systems Control Process

Figure 4.17 describes the detailed activities of this process. The process begins with the identification of the assessment results of each process phase and risk factors. These identified results conduct trade-off for selecting risk-handling options through the analysis of the life cycle cost, system and cost effectiveness, environmental impacts and quantification of risk factors. The risk handling options are controlled by the various management methods, such as data, configuration, interface, RAMS and performance based progress as shown in Figure 4.17 (BS IEC/ISO 26702, 2007).

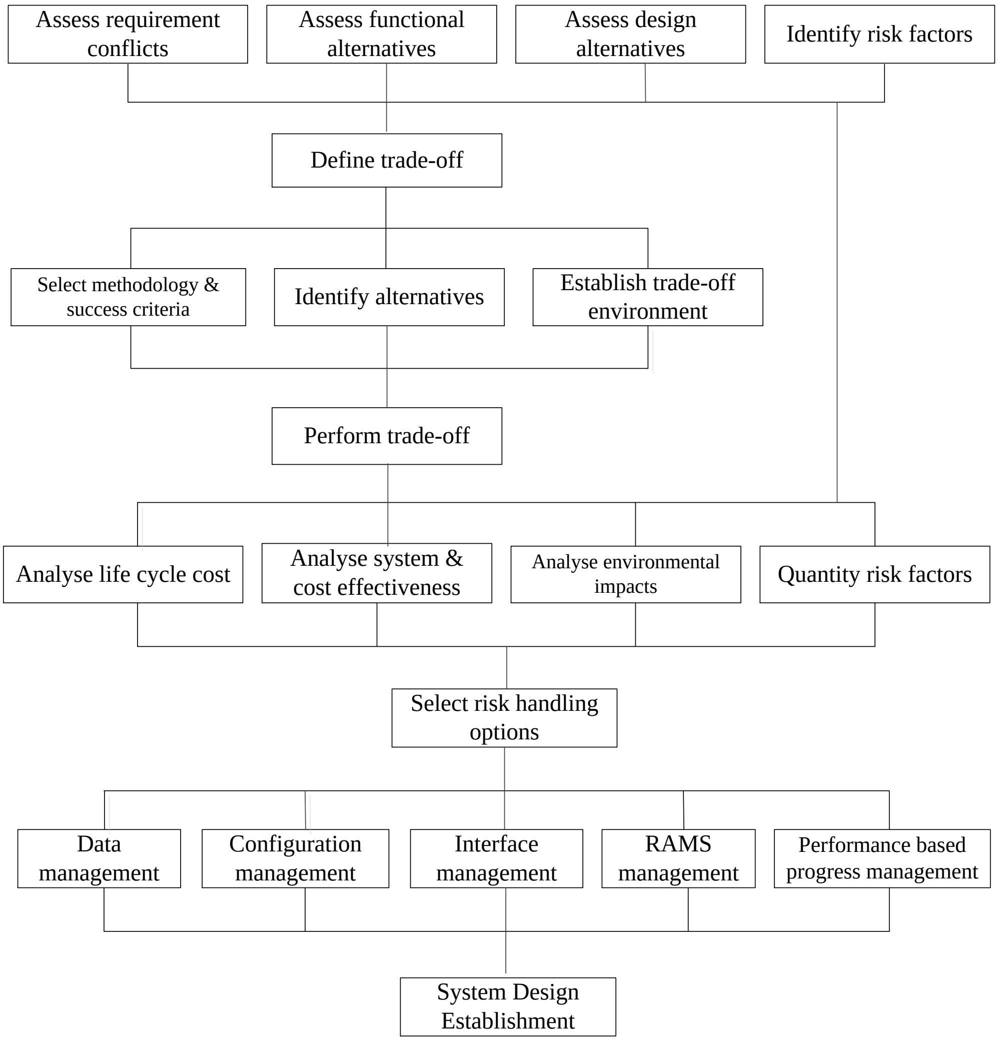

Assess requirement conflicts
Assess functional alternatives
Assess design alternatives
Identify risk factors
Define trade-off
Select methodology & success criteria
Identify alternatives
Establish trade-off environment
Perform trade-off
Analyse life cycle cost
Analyse system & cost effectiveness
Analyse environmental impacts
Quantity risk factors
Select risk handling options
Data management
Configuration management
Interface management
RAMS management
Performance based progress management
System Design Establishment

Figure 4.17 Systems Control Process Activities

4.4 Development of Risk Based RAMS Management Process

As described in Figures 4.8 and 4.17, railway systems engineering management focuses on the control of railway risk handling options which are determined through the trade-off of life cycle costs, system and cost effectiveness, quantitative risk factors and environmental impact. RAMS management will also focus on the control of RAMS characteristics for the risk handling options. Therefore, the risk assessment process will be a core part of the RAMS management process to provide a complete understanding of railway risks which are included in the system and operational contexts. The life cycle costs, the system and cost effectiveness which support the selection of risk handling options can be considered as an integrated part of RAMS management, but full attention will be devoted to the railway RAMS management for the assessment and control of risk handling options. Figure 4.18 describes a proposed risk based RAMS management process; it consists of four process phases: requirement definition phase, risk assessment phase, RAMS control phase and monitoring and review phase (An, 2005; BS EN 31010, 2008).

The risk based RAMS management process will cover all perspectives related to the assessment and control of railway risks in order to provide the rational decision-making that will minimise, reduce, eliminate, even avoid or share the evaluated railway risks. The requirement definition phase determines the RAMS risk design requirements and their acceptance criteria. The risk assessment phase is implemented to identify, analyse and evaluate the railway risks. Firstly, risk identification is a phase that determines all potential risk factors and develops the models needed. Risk analysis is a phase that quantifies the failure severity and frequency of the failure scenario models. Moreover, risk evaluation is a phase that determines the risk level of a failure consequence using a risk evaluation matrix. The multitude of the risk level should require the RAMS management for the improvement of the design or the development of the maintenance policy and the process activities should be monitored and reviewed continuously as shown in Figure 4.18.

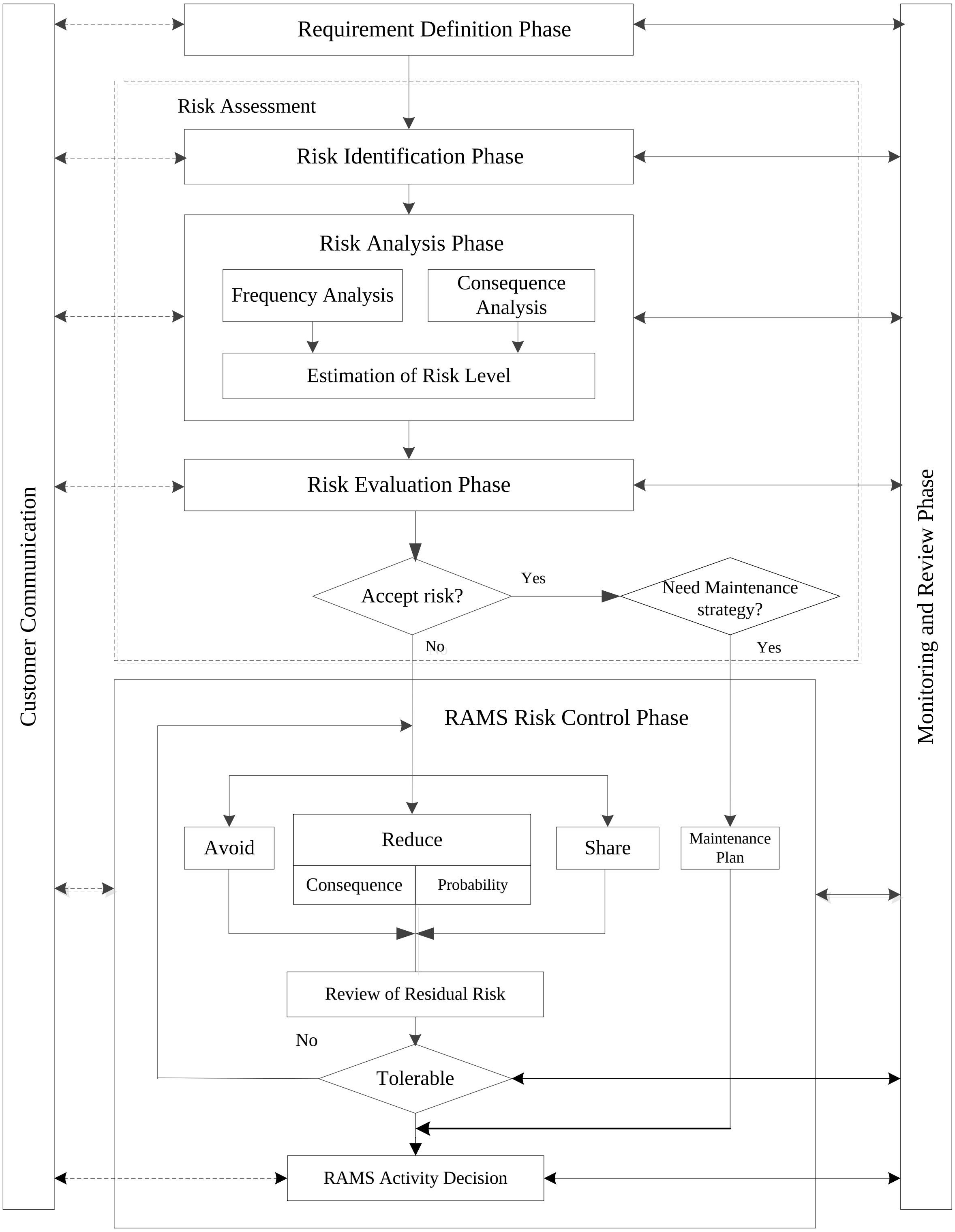


Figure 4.18 Proposed Risk based RAMS Management Process

4.4.1 Requirement Definition Phase

This phase is implemented in the requirement definition phase of the systems engineering process. Figures 4.9 and 4.10 are fundamental in the application of this process phase. The process involves identifying the need and implication of RAMS management in the railway systems engineering through a feasibility study, and defines the RAMS requirements and their acceptance criteria. The RAMS requirements should be defined and specified by different system hierarchy levels: operational design level, functional design level and physical design level. The following typical requirements may be needed in this phase (An et al, 2006; BS IEC/ISO 26702, 2007):

- Design constraints: e.g. sets of rules and standard regulations;
- Operational scenarios and operational effectiveness;
- System boundaries, operational environments and life cycle process;
- Functional requirements; deterministic and/or probabilistic RAMS requirements and;
- RAMS acceptance criteria.

4.4.2 Risk Identification Phase

The risk identification phase is conducted in the functional definition and the allocation phase of the systems engineering process. Figures 4.11 and 4.12 are fundamental processes needed for successful achievement of risk identification. The identification involves identifying the following activities: (1) the sub-functions and their performance, (2) all possible failure modes, causes and effects that may be included in the sub-function states and modes and data flow, last of all (3) determining safety functions and their monitoring functions.

The purpose of this phase is to produce a comprehensive list of railway risks, based on all possible failure modes that may affect the railway service, and to determine the scenarios for all failure effects and causes. Railway risks can be identified and evaluated by the following methods (BS EN 31010, 2008):

- Evidence based approach, for example, checklists and past data;
- Systematic teamwork approach, and;
- Inductive step by step approach.

In this process, typical risk identification techniques, such as brainstorming, checklists, what-if, failure mode and effect analysis (FMEA) or hazard and operability study (HAZOP), can be deployed, depending on the analytical objectives. However, the FMEA technique has been applied most commonly because it is very effective in identifying all possible failure modes and it can practically support other analysis techniques practically to represent the logical structures or the expert opinions, such as ETA, FTA and Fuzzy Logic Analysis approach (An, 2005).

4.4.3 Risk Analysis Phase

Risk analysis phase is conducted in the design definition and synthesis phase of the systems engineering process. Figures 4.13 and 4.14 are a basis for implementing this phase. The risk analysis involves estimating the frequency of the failure consequence for design solution alternatives by using the identified failure data. The risk analysis process begins with the identification of failure severities of the failure consequences in order to quantify them. If the collected failure data cannot be quantified, qualitative approaches should be considered. However, if the level of the identified uncertainty is very high, the specific risk analysis methods or combined methods may be considered in order to quantify the level of failure consequence, for example, FMEA, FTA, ETA etc. (An, 2005).

As the systems engineering design stage progresses step by step, more failure data and information sources related to railway risks may be collected with the more detailed failure data and information sources, the failure cause analysis required for the failure frequency can be implemented in more detail. The FTA technique is an excellent technique for the qualitative and quantitative analysis of the failure causes in which it can analyse the roots of the failure causes, their relationship and their interaction. The basic failure causes that may lead to top events are identified by the cut sets analysis using the Boolean algebra rules. The minimal cut sets identified by the cut set analysis must have been balanced for the system design architecture, and the quantitative analysis can be conducted by failure probability or failure rate (Ericson, 2005; BS EN 61025, 2007).

4.4.4 Risk Evaluation Phase

This phase is conducted to determine the overall risk levels with a combination of the failure severity of the failure consequence and its frequency to occur. The risk evaluation provides a good understanding of railway risks to support the decision-making for RAMS management. The railway risk evaluation is a process of comparing the analysed railway risk levels with the defined risk criteria to determine the importance of the level and type of the railway risk. Risk evaluation is conducted by a defined risk matrix, which is a matrix that is used to define the various levels of risk as the product of the probability and severity categories (BS ISO/IEC 31010, 2008).

4.4.5 RAMS Risk Control Phase

This phase is conducted in the systems control phase of systems engineering management. Figures 4.16 and 4.17 are the basis for carrying out these process activities. The RAMS risk control phase aims to select risk-handling options appropriately by the RAMS acceptance criteria, as shown in Figure 4.16. The cost or system effectiveness analysis is based on the RAMS risk control within the tolerable risk level. The RAMS control can be implemented by the five actions as shown in Figure 4.18 (BS IEC 62198, 2001):

- Avoid the risk altogether;
- Decrease the failure probability of occurrence;
- Reduce the failure consequences;
- Transfer or share the risk and;
- Maintain the risk and make maintenance plans and strategies.

4.4.6 Monitoring and Review Phase

As shown in Figure 4.18, all process stages are monitored and reviewed to ensure that management actions are effectively taken. It makes sure that the proper procedures are selected and adequate information is collected throughout the RAMS management process. The verification activities of Figure 4.17 are the basis of this process and these methods. It should be noted that the system is evolving and becomes more complex, which may mean that the system is exposed to new risks as the system engineering process progresses over time. Accordingly, the monitoring and review process can track the changes that the system may have undertaken (Berrado et al, 2010; BS EN 31010, 2008).

4.5 Summary

This chapter has presented the methods for integrating RAMS management into railway systems engineering, such as the development of railway RAMS management systems, the establishment of the railway systems engineering process and its activities, the development of RAMS management process etc.

Firstly, this chapter provided a proposed framework for developing railway RAMS management systems including the establishment of management principles, the determination of management elements, the integration of management elements as a system, and the development of the technical management process. This chapter provided a process based railway RAMS management systems that can be applied to a railway systems engineering design phase to direct RAMS management policies and objectives, to coordinate RAMS management functions, and to control RAMS management activities.

Furthermore, railway systems engineering process and its process activities were established through the combination of several logical block diagrams to provide the fundamentals of the RAMS management functions and activities. The railway systems engineering process consists of the systems management that implements the trade-off of risk, system, cost and progress and the control of risk handling options as well as the technical engineering process that defines, analyses and evaluates the requirements, functions and design.

Finally, the risk based railway RAMS management process were proposed to focus the control of all possible railway risks within the acceptable range by the RAMS management. The risk-based RAMS management process provides RAMS requirement definition, risk identification, risk analysis, risk evaluation, RAMS risk management and monitoring, based on the established systems engineering process phase.

Systems engineering and RAMS management are respectively new engineering management concepts to railway organisations. Therefore, there are many difficulties in establishing the systems engineering and RAMS management at once, but the models and processes proposed in this chapter will help railway organisations to gradually establishing and implementing RAMS management at the early system concept design phase.

Chapter 5

DEVELOPMENT OF FMEA-FTA BASED RAILWAY RAMS RISK ASSESSMENT TECHNIQUE

5.1 Introduction

The engineering of the mission and safety critical systems, such as railway and aeroplane, has to focus the control of all potential hazards which may pose a threat to system performance as a whole as stated in Chapter 4. Thus, the risk assessment of the hazards is the main focus of RAMS management. The railway hazards are assessed by the qualitative, quantitative or semi-quantitative methods to determine the risk level of the hazards, which is determined by the combination of the failure severity and frequency of the failure consequence. The failure severity, as a qualitative assessment parameter, is determined by the bottom-up approach method. The failure frequency, as a quantitative assessment parameter, is evaluated by the top-down approach method. Therefore, the risk assessment of railway systems requires the various types of risk assessment techniques that satisfy the above stated methods (An, 2005).

Many risk assessment techniques have been developed, and the techniques have widely applied to the mission and safety critical systems. Railway industry has also studied and tried the application of the various techniques appropriate to the risk assessment of railway hazards for the long time. Most studies for the risk assessment technique have emphasised the individual application of the risk assessment techniques. However, their individual application may not meet the precise analytical objectives of the risk assessment through the entire system engineering process. Accordingly, the combination of various different risk assessment techniques has been required, but the practical application methods have not been provided. Therefore, this chapter presents the method which combines risk assessment techniques, depending on the analytical objectives, information and data available and the systems engineering design phase (Zhou et al., 2001; An, 2005).

This chapter consists of four sections to present the risk assessment method of railway hazards. Section 5.2 discusses the application of FMEA-FTA techniques to the railway risk assessment and their combination models. Section 5.3 presents the FMEA-FTA based railway risk assessment process that is applicable to cover all phases of systems engineering process. This chapter is concluded with a brief summary in Section 5.4.

5.2 Development of FMEA-FTA based Railway Risk Assessment Model

5.2.1 Railway Risk Assessment Technique

All railway risks that threaten the performance of RAMS characteristics designed to achieve the operational objectives are the central focus of RAMS management, which is supported by the processes and techniques appropriate to the nature of railway risks. Many inherent risks identified from railway systems and the challenges which have been posed from railway development projects must be continuously improved from the early stage of system concept design. As stated in this thesis, railway risks have a great potential to cause injury and/or loss of life of staffs or passengers, to cause environmental degradation, to damage to railway property or freight and to impose other adverse impacts upon the various operational conditions. Therefore, railway risk assessment requires a systematic approach with appropriate technique and process to successfully control all potential railway risks in the systems engineering design phases.

Many typical techniques are currently being attempted and studied to assess railway risks explicitly and effectively, for example, Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Failure Mode and Effect Analysis (FMEA), Failure Mode, Effect and Criticality Analysis (FMECA), Hazard and Operability Analysis (HAZOP), Fuzzy Logic Analysis (FLA) etc., as reviewed in Chapter 3. However, the application of the risk assessment techniques to the systems engineering process have been not provided. The typical risk assessment techniques were generally developed by the specific analytical objective needed in the systems engineering process phase or data available; they have inherently specific characteristics as reviewed in Chapter 3. Therefore, risk assessment techniques shall be appropriately used by their analytical objectives, data and information available and system design phase.

The increasing complexity of railway systems, their risky nature and the limited availability of information and data resources require various analytical methods and techniques as occasion demands of the systems design phase. It is essential to appropriately combine the risk assessment techniques needed. Therefore, the combination of FMEA and FTA techniques is proposed and its application as the basic technique for a railway risk assessment is described as below.

5.2.2 FMEA and FTA Risk Assessment Techniques

In Chapter 3, the features of FMEA and FTA techniques were discussed in details: i.e., analytical objectives, applications, advantages, disadvantages etc., which will be reviewed again to demonstrate the need of the combination of FMEA and FTA.

FMEA is a useful technique for risk assessment and it has been effectively used for the detailed failure analysis of the system which can cause the failure consequences that affect railway systems. The analysis procedure of FMEA can also be applied as an essential engineering design process to define all potential failure modes and effects of a system. However, FMEA has several challenges to be overcome in the risk assessment of large-scale, complex systems that have multi-functions and safety functions like railway systems. This technique has the difficulty in the quantification and logical expression of the detailed relationship of the system elements to judge the defects or weak points in the system engineering design phase (BS EN 60812, 2006; BS ISO/IEC 26702, 2007).

When FMEA is applied to the analysis of the system that has several hierarchy levels with many redundancy structures, it becomes very complicated and even causes misunderstanding or errors. FMEA cannot effectively represent the relationship between individual and group of failure modes or causes, so it is difficulty in supporting the system design process adequately. Furthermore, the deficiency of FMEA is clearly shown in the interactive expression of components in the system engineering design. However, such deficiencies of FMEA can be overcome and further complemented by the integration of two or more different techniques that can logically express the relationship of system components, for example, FTA, ETA etc. FTA has been recommended most commonly as the integration technique of FMEA to effectively design the high safety risk nature of railway systems (BS EN 60300-1, 2004).

FTA can effectively trace the low-level failure causes of a high-level failure consequence by building a logical and graphical fault tree and providing a quantitative and qualitative minimal cut set representations of the fault tree. FTA is a useful technique to model the scenarios of the failure causes, especially single failure points which directly lead to major safety accidents. Therefore, FTA can be used in the identification and design of safety functions and their monitoring functions.

FMEA is a systematic, inductive risk assessment technique which is used for the qualitative assessment of failure consequences, whilst FTA is a deductive technique which is most often used for the quantitative assessment through the logical analysis of failure causes. As stated in Chapter 4, systems engineering design process requires various risk assessment methods: an inductive and/or deductive approach, including qualitative, quantitative and/or semi-quantitative assessments to achieve the engineering design objectives effectively. Therefore, the combination of FMEA and FTA can form a useful risk assessment method to achieve all of such analytical requirements, depending on the system design phase (Gofuku et al., 2006).

5.2.3 FMEA and FTA Based Risk Assessment Models

As stated in Chapter 3, railway risk is defined by the combination of the severity degree of a failure consequence and its frequency or probability. The railway risk assessment requires the clear answers for the following four questions (see diagram) to determine the levels of the failure severity and frequency. Therefore, a process that determines the levels of railway risk can be represented as shown in Figure 5.1. Each step will require the selection of the appropriate risk assessment techniques that can satisfy the given questions.

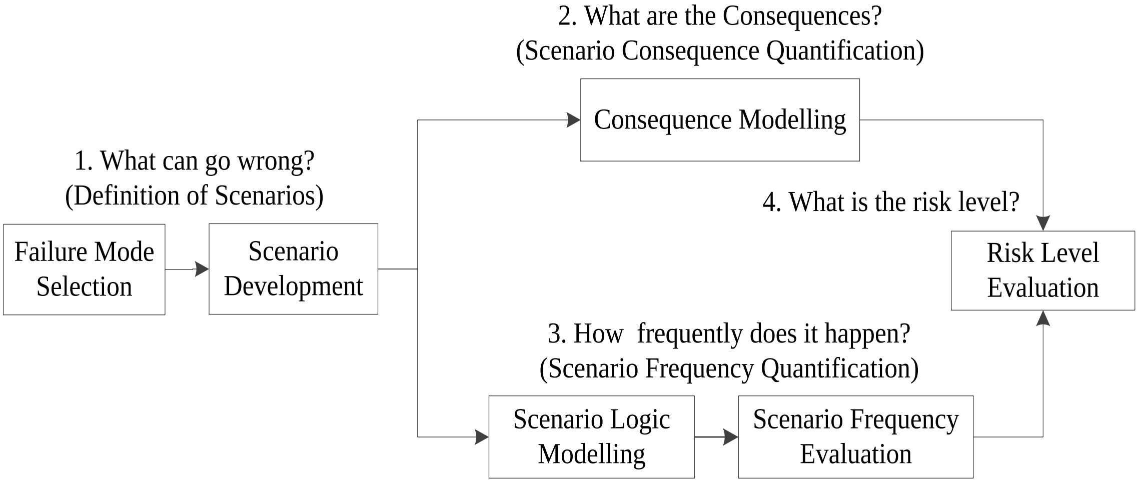

2. What are the Consequences?
(Scenario Consequence Quantification)
Consequence Modelling
1. What can go wrong?
(Definition of Scenarios)
4. What is the risk level?
Failure Mode Selection
Scenario Development
Risk Level Evaluation
3. How frequently does it happen?
(Scenario Frequency Quantification)
Scenario Logic Modelling
Scenario Frequency Evaluation

Figure 5.1 Concept of Railway Risk Assessment

Figure 5.2 shows the proposed risk assessment technique based on FMEA-FTA appropriate to the model of Figure 5.1. The FMEA technique is used for the qualitative failure analysis of all system elements, such as all possible failure modes, their consequences and causes, and the scenario development of the failure consequences and causes and it applies the bottom up approaches to the failure analysis in order to answer the questions 1 and 2.

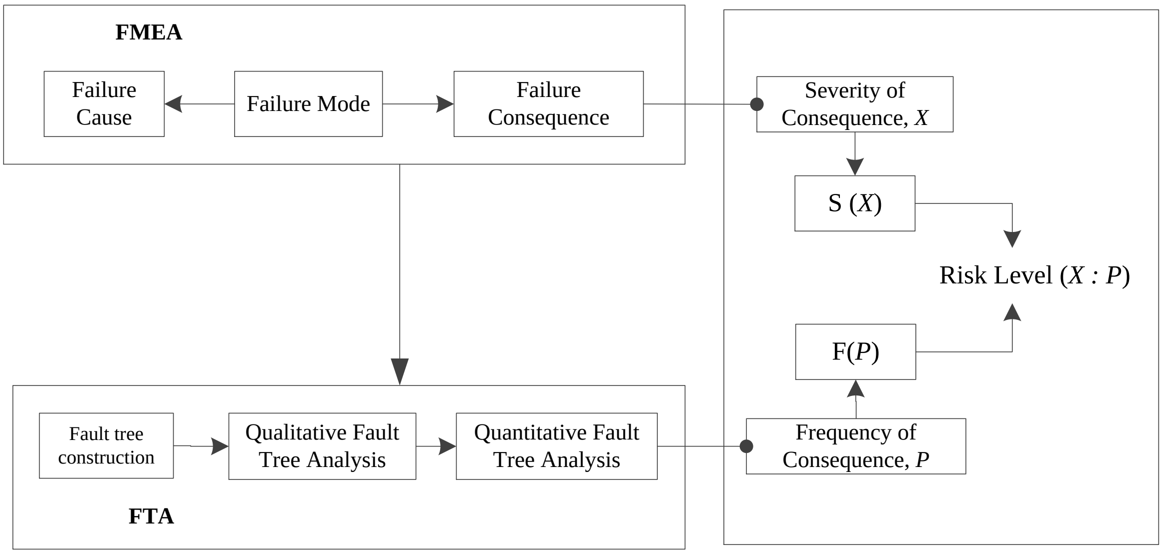

FMEA
Failure Cause
Failure Mode
Failure Consequence
Severity of Consequence, X
S (X)
Risk Level (X : P)
F(P)
Fault tree construction
Qualitative Fault Tree Analysis
Quantitative Fault Tree Analysis
Frequency of Consequence, P
FTA

Figure 5.2 Concept of FMEA-FTA based Railway Risk Assessment

On the other hand, FTA is used for the quantitative analysis of the failure consequences through the logical analysis of the failure causes, which are analysed by the logical structures of the fault tree, Boolean algebra rules, the developed scenarios of failure causes and the top-down approach in the failure analysis to answer the question 3.

Figure 5.3 shows the combination method of FMEA and FTA techniques at any analytical point of a risk. The first performs the FMEA analysis for all system elements and the results of the FMEA analysis are effectively supported by the fault tree construction, which performs the qualitative and quantitative analysis of the failure tree by using Boolean algebra rules and probability laws. However, the purpose of the combination is differently applied in the system engineering design phase as shown in Figures 5.5 and 5.6.

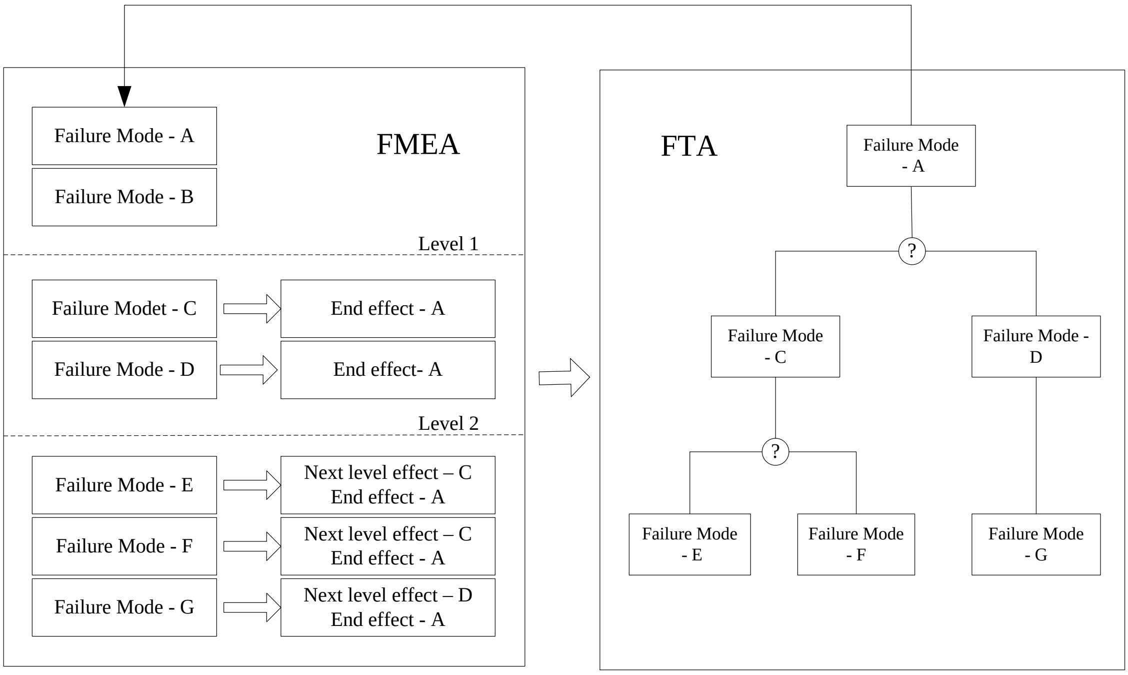


Figure 5.3 FMEA and FTA Combination Model

The FMEA and FTA combination model of Figure 5.2 can be applied by two methods: top-down approach and bottom-up approach, depending on the systems engineering design phase as shown in Figure 5.4. As stated in Chapter 4, the subsystem definition phase is performed to define the functional architecture of the subsystems. Accordingly, the failure analysis is conducted as a top-down approach to trace the root failure causes in the objective for identification and establishment of the safety and their monitoring functions. The component definition phase is to define the physical design architectures. Thus, the failure analysis is conducted as a bottom-up approach to trace the failure consequence scenarios quantitatively. Figure 5.4 describes FMEA-FTA based risk assessment approach for a failure hazard. However, the FMEA-FTA combination models can apply two approaches at the same time as shown in Figure 5.4. Therefore, in each design phase, the analysis of the failure consequences and causes can be applied at once.

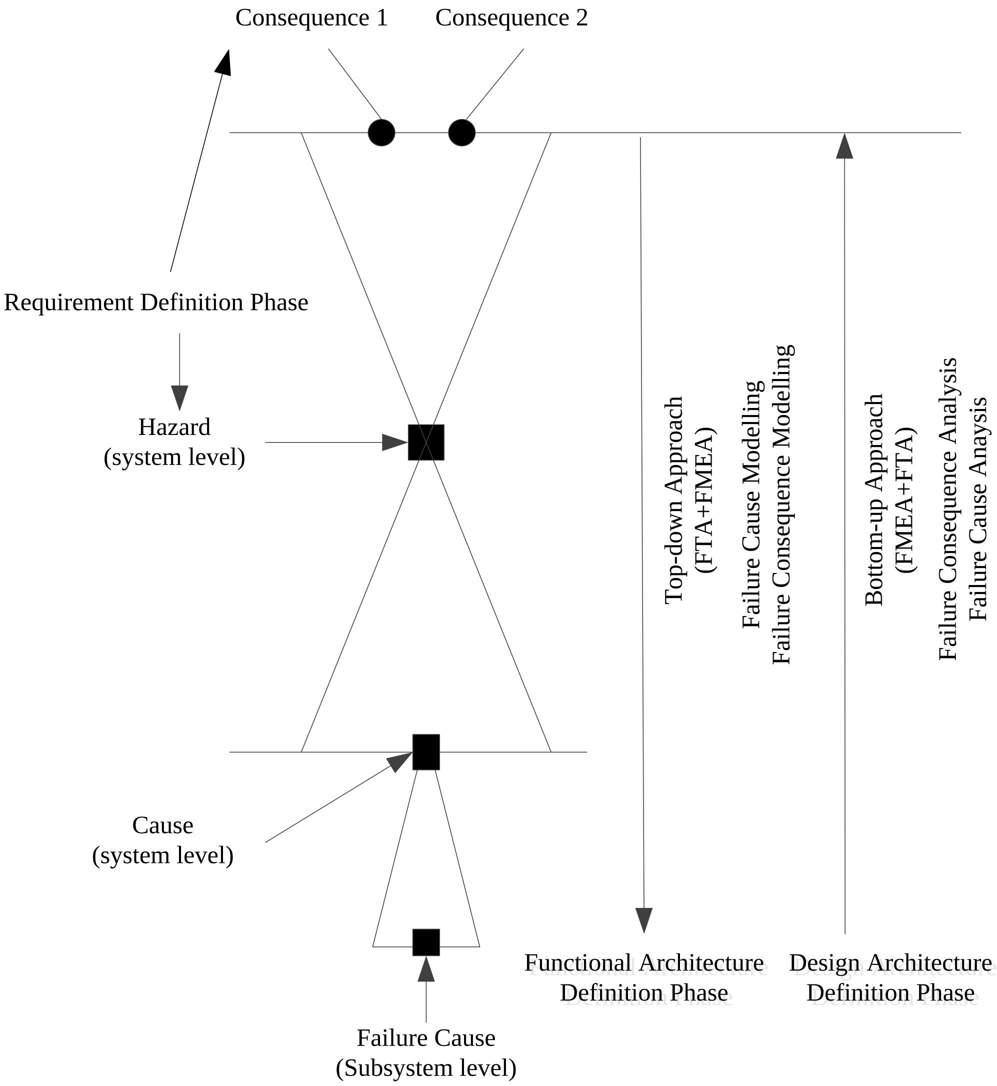


Figure 5.4 FMEA and FTA based Railway Risk Assessment Approach Model

5.2.3.1 Top-down Risk Assessment Model

Figure 5.5 shows the principle of an integrated FTA-FMEA approach model and it is applied for the top-down (or backward) risk assessment in the systems engineering process. In this model, FTA has an active role as the main assessment technique to trace the root of a failure cause, while FMEA is for all possible failure modes, causes and effects and the results of FMEA analysis support the FTA to continuously expand the fault tree model until the roots of failure causes are reached, and they also support the development of the modelling and severity classification of failure consequences. Figure 5.5 describes the combined model of FTA-FMEA techniques.

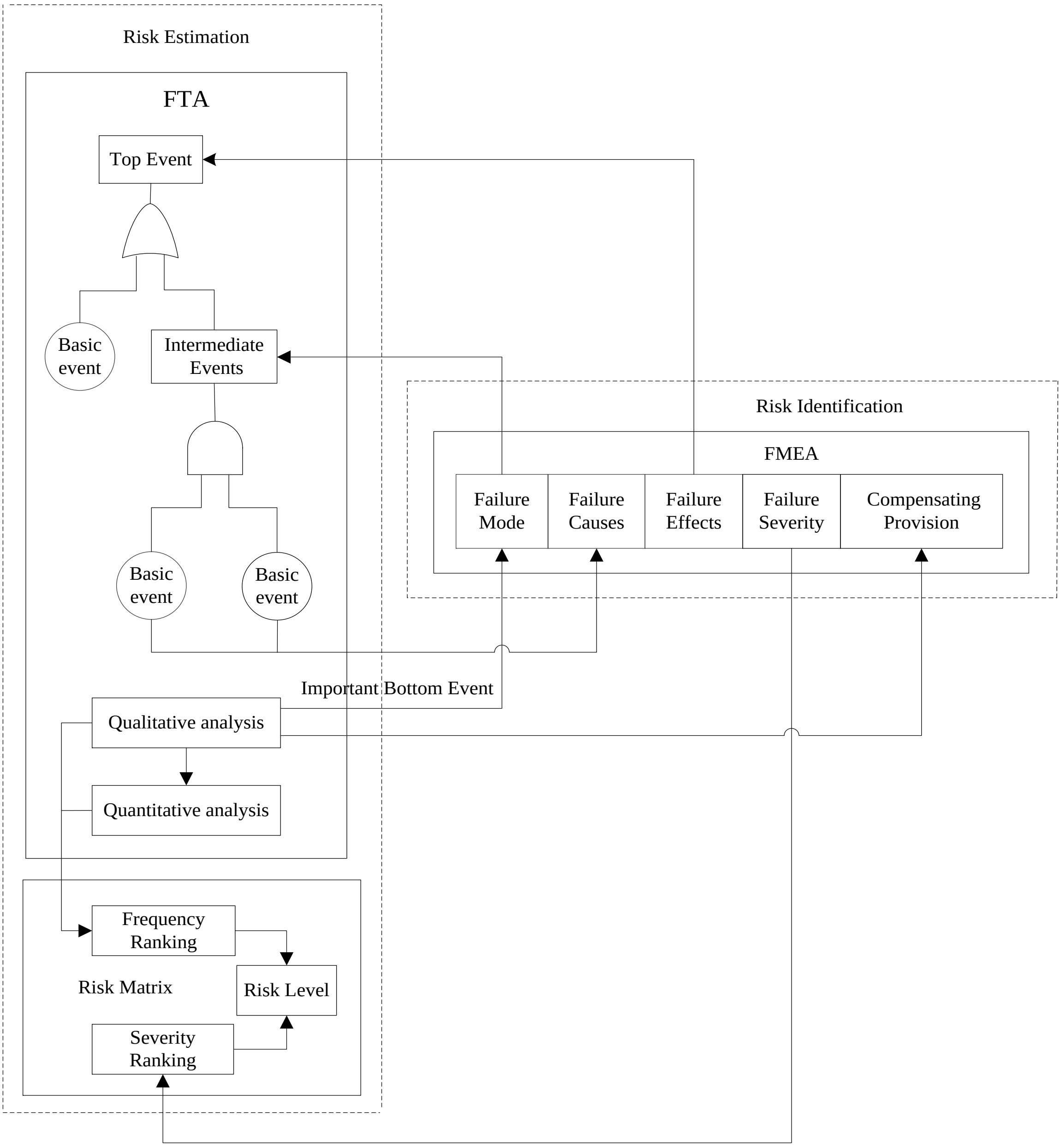


Figure 5.5 FTA-FMEA based Top-down Risk Assessment Model

The FTA-FMEA model starts by selecting a top event. The top event can be determined by various analytical methods: preliminary hazard analysis (PHA), hazard and operability analysis (HAZOP), hazard log lists, safety requirements etc. at different design phases, but the selected top events should be analysed by FMEA because it can determine all analytical items that are needed to assess risks and it supports the construction of a fault tree and the modelling of the failure consequence scenarios.

The important bottom events that are identified from the qualitative fault tree analysis in the system design phase are applied as the failure modes to conduct the FMEA analysis of the next system level, as shown in Figure 5.5. The compensating provision is very important to establish the functional architecture. This model is very useful in supporting the design and analysis of adequate functional structure (subsystems), as it has a great advantage for the identification of safety functions and safety monitoring functions, as described in Chapter 4.

5.2.3.2 Bottom-up Risk Assessment Model

Figure 5.6 shows the principle of an integrated FMEA-FTA approach model, which is applied for the bottom-up (or forward) approach in the failure analysis of the design architecture of the railway system. In this model, FMEA is deployed as the main analysis technique and FTA supports the FMEA analysis for qualitative and quantitative analysis of the failure causes in more detail by providing the logical structure of system design and the quantified evaluation of failure causes.

FTA analysis is in turn conducted by the severity ranking of the failure effects at any system design phase to identify the failure causes quantitatively. The failure modes are used as intermediate events in the fault tree, as shown in Figure 5.6. In this model, FTA is implemented more comprehensively to provide the compensating provisions for failure causes to support the system design and maintenance policy. This approach model can be applied from component to system level in the design definition phase as stated in Chapter 4.

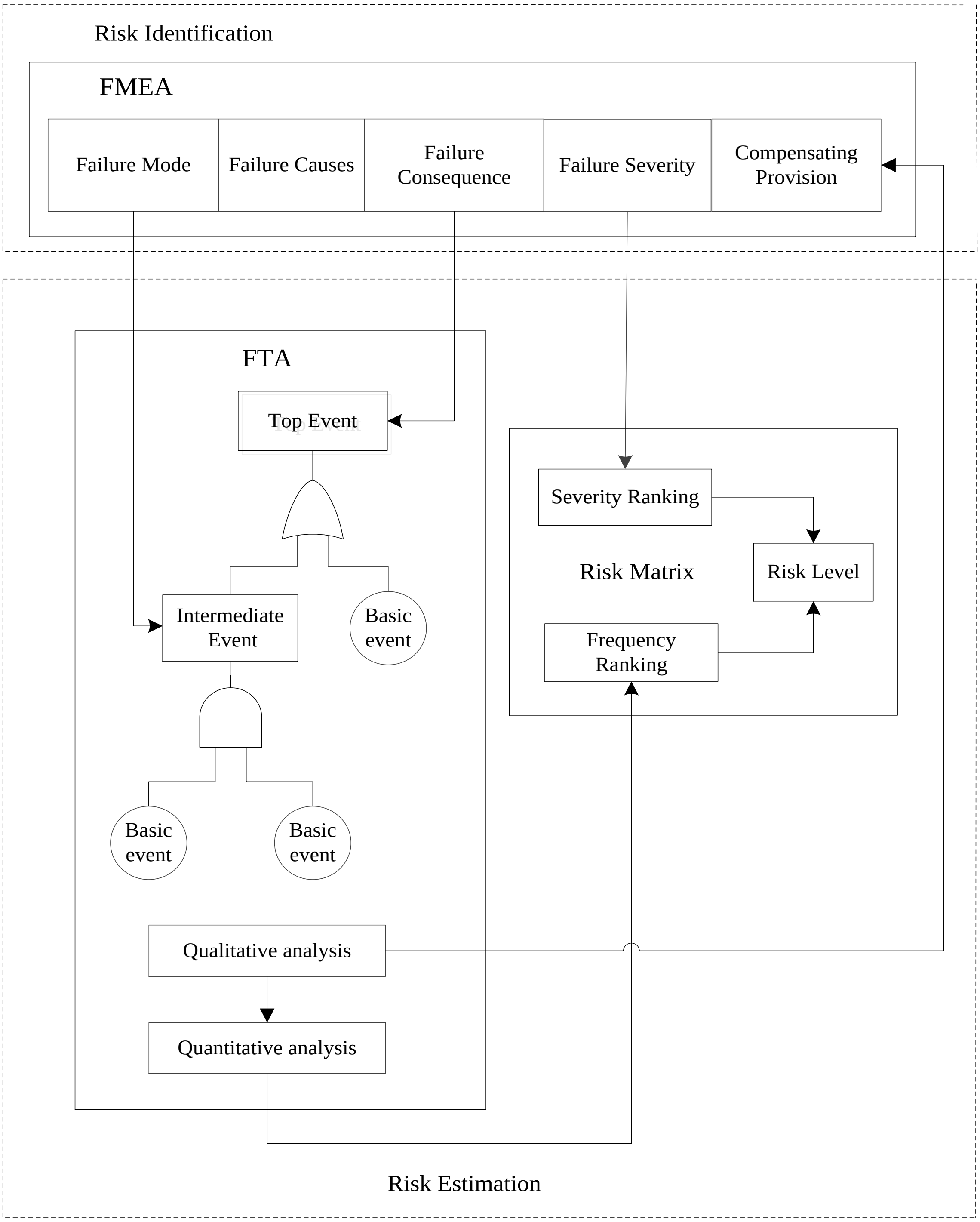


Figure 5.6 FMEA-FTA based Bottom-up Risk Assessment Model

5.3 Development of FMEA-FTA based Railway Risk Assessment Process

As stated in Chapter 4, RAMS management shall have a process to identify and assess all potential hazards and the relevant risks in the system engineering process and to provide the rational and basic information needed in determining the appropriate application of risk mitigation and elimination, and/or the control of risk measures. An effective risk assessment process will include all aspects related to railway RAMS risks in order to provide the rational decision-making that minimises, reduces, or even eliminates the railway risks involved through RAMS management. Therefore, risk assessment process will include the sufficient methods and techniques to demonstrate that failure modes with all potentials and pertinent measures applied to conform the level of risks to As Low As Reasonably Practicably (ALARP) (Umar, 2010; An et al., 2007).

The proposed railway risk assessment process based on FMEA and FTA commences with identifying the need of RAMS management and determining the RAMS requirements through the comparison and analysis of the relevant information and data collected from the past incidents and accidents of similar systems. The RAMS requirements are established with reference to statutory regulations, product deterministic life, failure modes as well as possible resultant failure consequences. However, the risk assessment of high complexity of railway system and its insufficient risk information and data source may require the combined use of risk assessment techniques to satisfy the use of experts or engineering judgement and the quantification of the risk evaluation concurrently in the system engineering design process. The important failure consequences are then further analysed through the progressive top-down steps from a system level to the components and then the bottom-up steps from components to the sub-systems and finally to a whole system level (Umar, 2010; An et al., 2004).

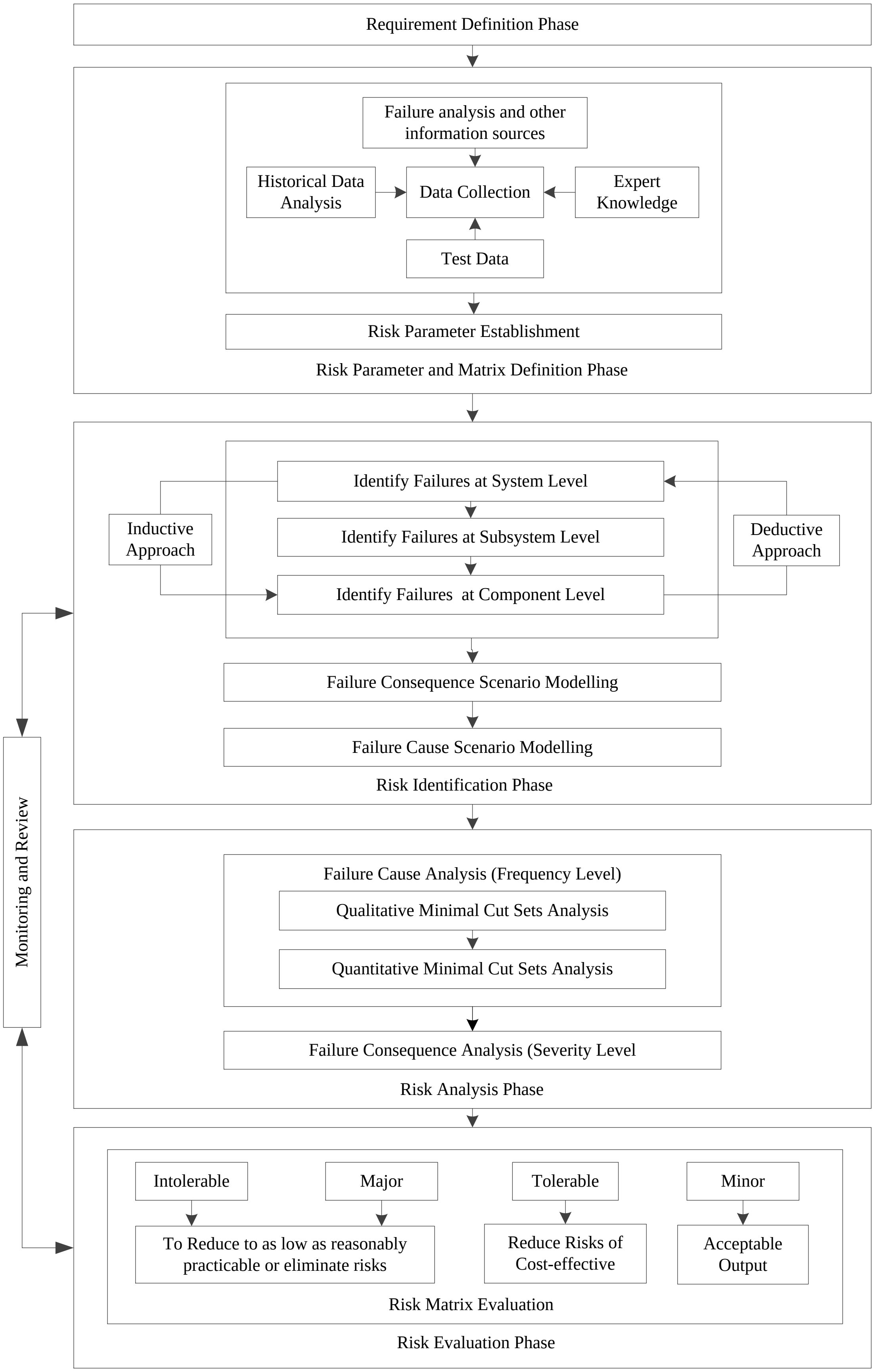

Requirement Definition Phase
Failure analysis and other information sources
Historical Data Analysis
Data Collection
Expert Knowledge
Test Data
Risk Parameter Establishment
Risk Parameter and Matrix Definition Phase
Identify Failures at System Level
Inductive Approach
Identify Failures at Subsystem Level
Deductive Approach
Identify Failures at Component Level
Failure Consequence Scenario Modelling
Failure Cause Scenario Modelling
Risk Identification Phase
Monitoring and Review
Failure Cause Analysis (Frequency Level)
Qualitative Minimal Cut Sets Analysis
Quantitative Minimal Cut Sets Analysis
Failure Consequence Analysis (Severity Level
Risk Analysis Phase
Intolerable
Major
Tolerable
Minor
To Reduce to as low as reasonably practicable or eliminate risks
Reduce Risks of Cost-effective
Acceptable Output
Risk Matrix Evaluation
Risk Evaluation Phase

Figure 5.7 Proposed FMEA-FTA Based Risk Assessment Process

5.3.1 Requirement Definition Phase

This process involves identifying the needs and implications of the RAMS management in the railway system engineering project through the feasibility studies, and then it defines the RAMS design solutions and their acceptance performance criteria through the definition of system boundaries, operational contexts, environments and life cycle processes. The RAMS design solution and acceptance criteria should be defined and specified by different system hierarchy levels: a system level, the subsystem level and component level comprising the system as shown in Figure 5.7.

The items need to be identified and defined in this phase (BS IEC/ISO 26702, 2007):

- Design constraints: e.g. sets of rules and standard regulations;
- Operational scenarios and measures of RAMS effectiveness;
- System boundaries, operational environments, and life cycle process;
- Functional requirements, deterministic and/or probabilistic RAMS requirements and;
- RAMS acceptance performance criteria.

5.3.2 Risk Parameter and Evaluation Matrix Definition Phase

After the RAMS requirements: i.e., design and acceptance criteria; system and operational contexts, are defined, the data and information needed for risk assessment are collected and analysed to establish the index and range of risk parameters, and to provide input for the risk assessment process.

5.3.2.1 Data Collection and Analysis

The second phase of the risk assessment process starts with the analysis of the collected data and information available to establish the index and range of a risk parameter and a risk evaluation matrix, and to provide an input to the risk assessment process. The data and information are collected from historical data, test data, expert knowledge and sources of other information, as shown in Figure 5.7.

The objectives of the collected data and information analysis are to identify the explicit understanding of all possible railway risks from the past accidents and incidents of similar systems, and to obtain a set of information from the collected data. If the data is not statistically accurate or the amount of data is insufficient, expert judgement and/or engineering decisions can be applied. The information and data identified and analysed can be used to determine the ranking of index parameter, and make up a qualitative indexing matrix (Umar, 2010). .

Many common statistical techniques can be applied to collect information and knowledge, for example, statistical data and information analysis, human experience and engineering knowledge analysis, conceptual mapping etc. Two or more of these techniques can be combined to overcome their inherent shortcomings and to reinforce their inherent environmental characteristics (An et al., 2007).

5.3.2.2 Establishment of Risk Parameters

The information and data that are identified from the collected data can be used to determine the index ranking and make up a qualitative indexing matrix. By the definition of railway risk, the proposed FMEA-FTA based risk assessment model requires two risk index parameters: a failure severity parameter and a failure frequency parameter of occurrence. This is to determine the risk levels of the failure consequences of components and their impact on the sub-systems and the railway level system and it also requires an evaluation matrix to determine the risk level (An et al., 2007; BS EN 50126-1, 1999).

(1) Failure Severity Parameters

The failure severity parameter (FSP) of a failure consequence describes the possible magnitude of the failure consequence for the system as a whole. The FSP can be expressed by the defined words to define the different terms as described in Table 5.1: for example, insignificant, marginal, critical and catastrophic. The failure consequence of the railway system can be separated into three consequence conditions: people, environment or railway service. Table 5.1 shows the FSPs which are considerable in the railway risk assessment to rank the possible magnitude of all failure consequences (BS EN 50126-1, 1999).

Table 5.1 Failure Severity Parameters

Severity category	Level	Consequence to Person or Environment	Consequence to Service
Catastrophic	4	Fatalities and/or multiple severe injuries and/or major damage to the environment	Whole system failure
Critical	3	Single fatality and/or severe injury and/or significant damage to the environment	Loss of a major system.
Marginal	2	Minor injury and/or significant threat to the environment	Severe system (s) damage
Insignificant	1	Possible minor injury	Minor system damage

(2) Failure Frequency Parameters

Table 5.2 describes the classification of the failure frequency parameter (FFP) of occurrence of all possible failure consequences to quantify the risk level. In general, frequent, probable, occasional, remote, impossible and incredible are suggested in the interational standards and literature, and their failure frequency between 100/year and 10^{-6} /year is defined as shown in Table 5.2 (Kim et al., 2008).

Table 5.2 Failure Frequency Parameters

Category	Level	Description	Frequency
Frequent	6	It is likely to occur frequently and will be continually experienced.	≥100
Probable	5	It will occur several times and can be expected to occur often.	100< to ≤ 1
Occasional	4	It is likely to occur several times and can be expected to occur several times.	1< to ≤ 10^{-2}
Remote	3	It is likely to occur at some time in the system life cycle and can reasonably be expected to occur.	10^{-2}< to ≤ 10^{-4}
Impossible	2	It is unlikely to occur but is possible and can be assumed that it may exceptionally occur.	10^{-4}< to ≤ 10^{-6}
Incredible	1	It extremely unlikely to occur and can be assumed that it may not occur.	<10^{-6}

(3) Risk Level

Risk level (RL) is commonly expressed quantitatively or qualitatively as shown in Table 5.3.

Table 5.3 Risk Level Parameters

Risk Classification	Risk Level	Risk Reduction/Control
Unacceptable	4	Risk shall be eliminated.
Undesirable	3	Risk shall only be accepted when risk reduction is impracticable and with agreement.
Tolerable	2	Risk is acceptable with adequate control and agreement.
Negligible	1	Acceptable without any agreement.

BS EN 50126-1 (1999) provides qualitative descriptors, such as negligible, tolerable, undesirable and unacceptable and BS EN 50129 (2003) provides RL for signalling system design. Table 5.3 shows the qualitative descriptor categories of risk level derived from ALARP[17].

5.3.2.3 Establishment of Risk Evaluation Matrix

Table 5.4 shows a risk estimation matrix which determines the level of the railway risk. The risk evaluation matrix includes the levels of FFP in the horizental axis and the FSP in the vertical axis, as shown in Table 5.4. The point at which each index parameter mutually meets is the RL of a failure consequence. For example, if the FFP is ‘frequent’ and the FSP is ‘insignificant’, then the risk level is determined as ‘undesirable (high risk)’. If the FFP is ‘incredible’ and the FSP of failure consequence is ‘catastrophic’, and then the risk level is determined as ‘negligible’, as shown in Table 5.4 (BS EN 50126-1, 1999).

Table 5.4 Risk Evaluation Matrix

Frequency Level		Risk Level			
Frequent	6	Undesirable	Intolerable	Intolerable	Intolerable
Probable	5	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	4	Tolerable	Undesirable	Undesirable	Intolerable
Remote	3	Negligible	Tolerable	Undesirable	Undesirable
Improbable	2	Negligible	Negligible	Tolerable	Tolerable
Incredible	1	Negligible	Negligible	Negligible	Negligible
		1	2	3	4
		Insignificant	Marginal	Critical	Catastrophic
		Severity Levels of Failure Consequence			

[17] As Low As Reasonably Practicable

5.3.3 Risk Identification Phase

As stated in Chapter 4, risk identification is generally performed after the functional architecture has been established. Therefore, the functional block diagram, such as SADT[18] or FAST[19] which was described in chapter 3, is essential for the identification of possible risks with other collected data and information. As mentioned in Chapter 4, risk identification is a process that systematically identifies all potential failure modes, failure causes and effects at different system hierarchy levels, for instance, from component level to sub-system level; it determines the failure consequences and causes affecting the performance of the whole system level, and then establishes their two models. Therefore, the risk identification is performed in three process stages: operational, functional and design definition process stage, as stated in Chapter 4. The operational definition phase is conducted to confirm the major risks and the functional definition stage is conducted by a top down approach to identify and compare risks, and the design definition and synthesis stage is conducted by a bottom up approach for an update of the risks identified in the above phase. The risk identification is consisted of the identification of failure modes, the analysis of their failure effects and causes, and the development of their failure effect and cause scenario models.

At this process phase, typical risk assessment techniques, such as brainstorming, checklist, what if and HAZOP, can be used together with FMEA to identify railway risks explicitly. The risk identification initially started from the system level and is continuously extended to component level. It is repeated again from component level and completed at the system level as shown in Figure 5.7. This phase develops the scenario modelling of the failure

[18] Structured Analysis and Design Technique
[19] Functional Analysis System Technique

consequences and failure causes to confirm the logical architectures of the system design (An et al., 2007; Niels Peter Hoj, 2002; BS EN 31010, 2008).

5.3.3.1 Development of Failure Consequence Scenario

The scenario development of failure consequences is to estimate the impacts on the situations or circumstances of the failure events, which have a range of the level of the different failure severity. The failure consequences are modelled to determine the failure severity of the entire outcomes of a failure effect, a set of failure effects or by judging from experimental studies or past data. The scenario development of failure consequences starts from the occurrence of an initial event to the final failure consequence, as shown in Figure 5.8. Both ETA and FTA, based on the results of FMEA analysis, can be applied to model the logical and graphical scenario development of the failure consequences, but as stated in Section 3.4.5 of Chapter 3, if FTA is used to model the failure consequences of the systems which have multiple safeguards, the scenario would be very complex and large. Therefore, the systems which have the multiple safeguards like railway system are modelled by ETA. Figure 5.8 depicts the methods that develop the scenario of failure consequences by ETA (Ericson, 2005).

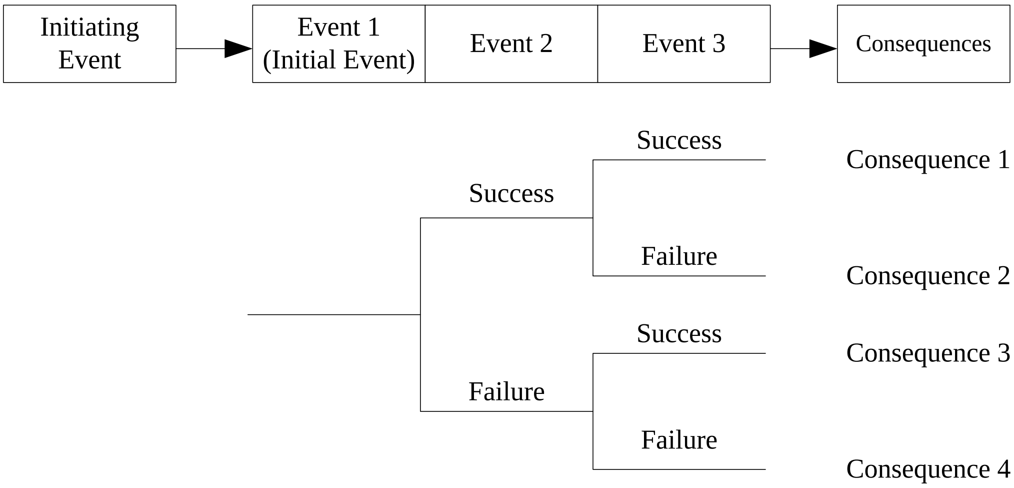


Figure 5.8 Development of Failure Consequence Scenario by ETA

5.3.3.2 Development of Failure Cause Scenario

Risk identification should be a structured method to identify all possible causes that lead to an undesirable system failure. It should organise the possible contributory factors into broad categories. However, not all possible failure causes may contribute to the actual failure because these can only be determined by collected data and empirical testing data. Accordingly, a fishbone diagram can more effectively judge all possible causes; so it is a very useful technique to represent and understand the relationship between failure causes leading to a failure consequence. Hence a fishbone diagram can effectively support FMEA analysis to identify the precise failure causes, and it can assist FTA analysis to model the failure cause scenarios as shown in Figure 5.9. The fishbone diagram can be easily converted as a fault tree. Figure 5.10 depicts a fishbone diagram that uses the factors affecting railway RAMS performance in the railway system, maintenance and operation conditions, provided from BS 50126-1 (1999).

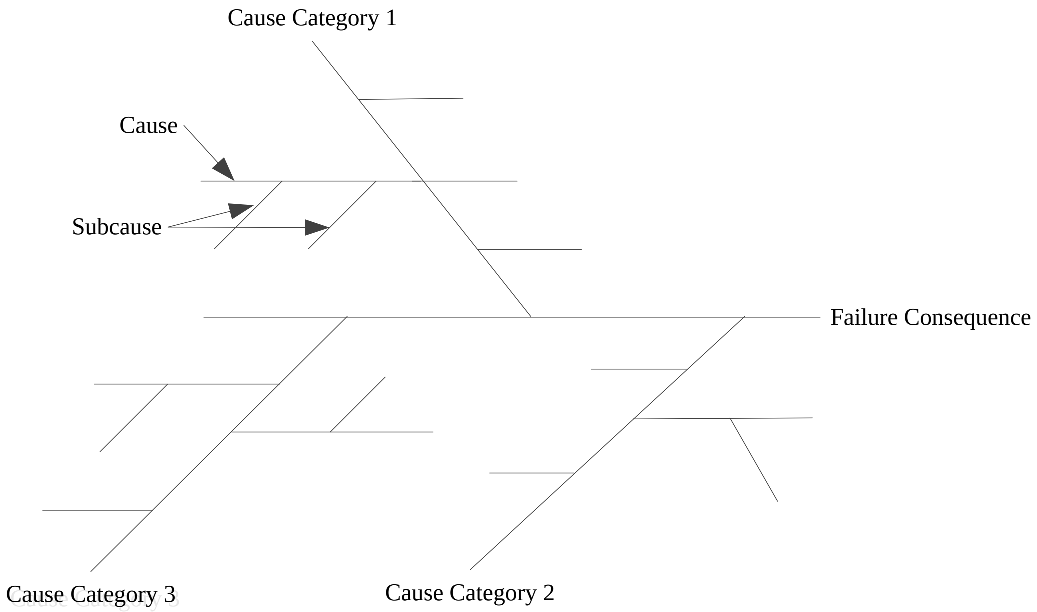


Figure 5.9 Establishment of Failure Cause by Fishbone Diagram

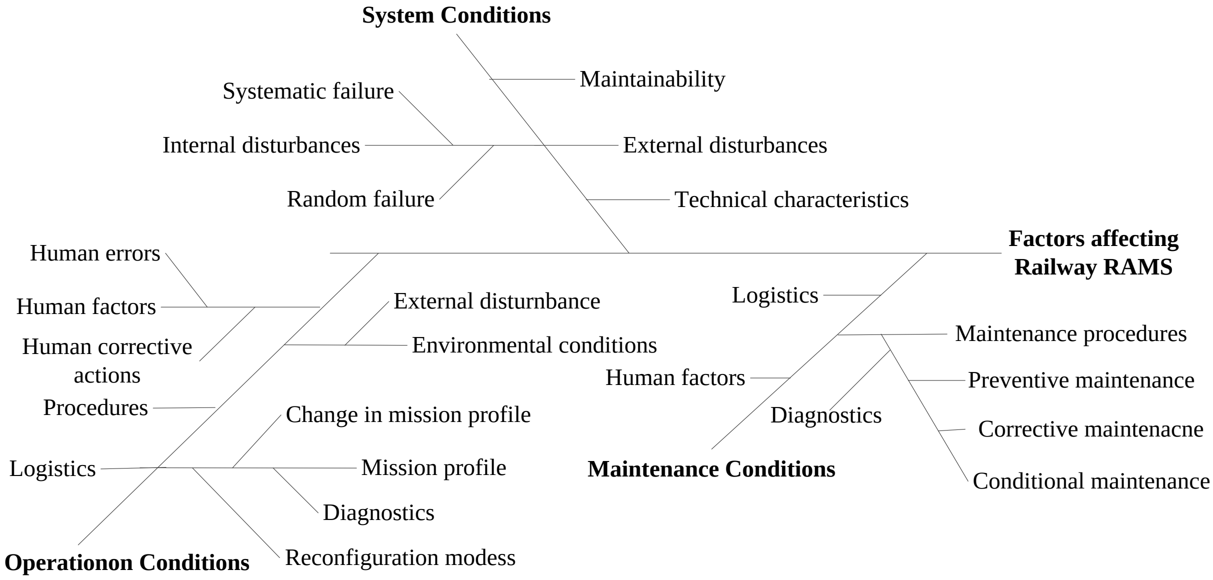


Figure 5.10 Factors affecting Railway RAMS

The scenarios of failure causes can be modelled by using a logical structure. The logical modelling is implemented by using a fault tree. The logical modelling is an iterative process that starts from a top event and it is continuously preceded through the tree structures until it reaches the root failure causes. This fault tree modelling is performed using the two steps as shown below:

Step 1: Top Event Determination

A fault tree is the symbolic representation of the system conditions that may cause a failure event so that the fault tree can identify the root failure causes of a failure event. The construction of a fault tree starts with identifying a top event and all events that lead to the top event. The top event is determined by three failure causes as shown in Figure 5.11.

Primary failure is an event of component failure within the design boundary, i.e. an event due to an inherent component characteristic. Secondary failure indicates a failure of a component outside the design boundary, i.e. a failure due to environmental or operational stress of a component. Command failure is an inadvertent operation for the component due to normal operation being commanded at the wrong time (Ericson, 2005; MIL-HDBK-764, 1990).

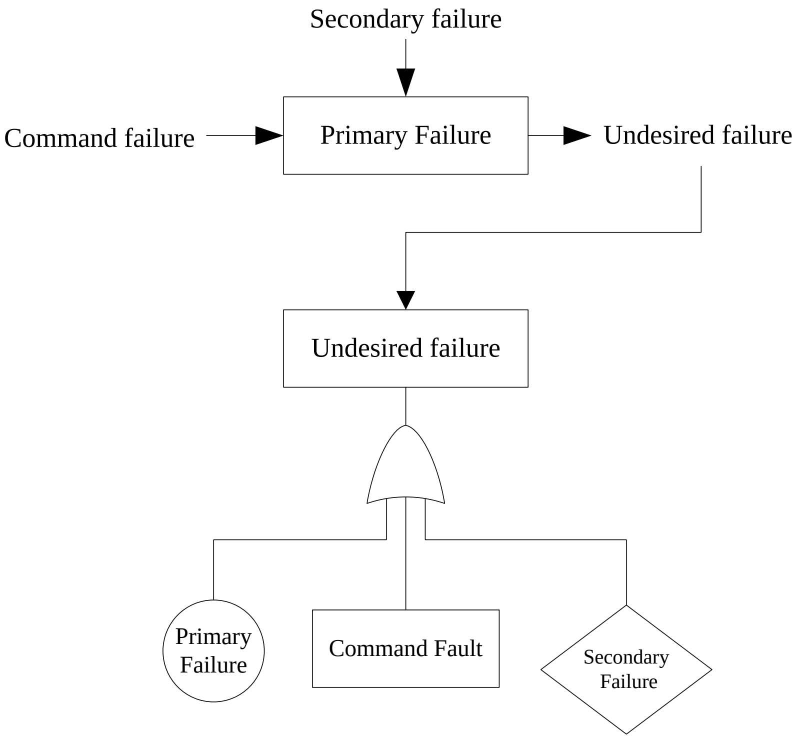
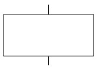
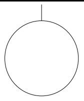
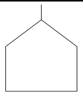
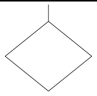
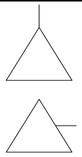
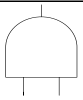
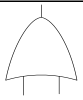
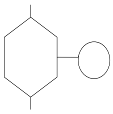


Figure 5.11 Fault Tree Construction Method

Step 2: Fault Tree Symbol Determination

The next step for the construction of a fault tree is to identify fault tree symbols. There are two kinds of symbols for building a fault tree: logic symbols and event symbols, as shown in Table 5.5. Logic symbols are for the interconnection of the failure events leading to the specific top event; the basic logic symbols are 'OR' and 'AND' gates. Event symbols represent the defined failure events by system hierarchy. Table 5.5 includes a brief description of the fault tree symbols that are often used.

Table 5.5 Definition of Fault Tree Symbols

Category	Symbols	Name	Description
Event Symbol		Top Event or Intermediate Event	Top event and intermediate event which describes the system fault, subsystem fault or higher level fault than the basic level fault.
		Basic Event	Basic event for the application of reliability information.
		House Event	Event which has happened, or will happen with certainty.
		Undeveloped Event	A part of the system that is yet to be developed or defined.
		Connecting Event	Gate indicating that this part of the system is developed in another part or page of the diagram.
Logic Symbol		AND Gate	Gate applies when all of the input events happen.
		OR Gate	Gate occurs when any of its input events happens.
		Inhibit Gate	Gate applies only if both the input events occur and one of them is conditional.

5.3.4 Risk Analysis Phase

Risk analysis is a process that quantitatively estimates the scenario of the failure causes and consequences developed in the previous phase to determine the risk level of failure consequence. Figure 5.12 shows the quantitative evaluation model of failure consequence, which is performed by the FTA analysis for the failure cause scenarios of the failure events. The evaluated levels of the severity and frequency of each failure consequence are applied to the risk evaluation matrix of Table 5.4 to determine the risk level (Ericson, 2005).

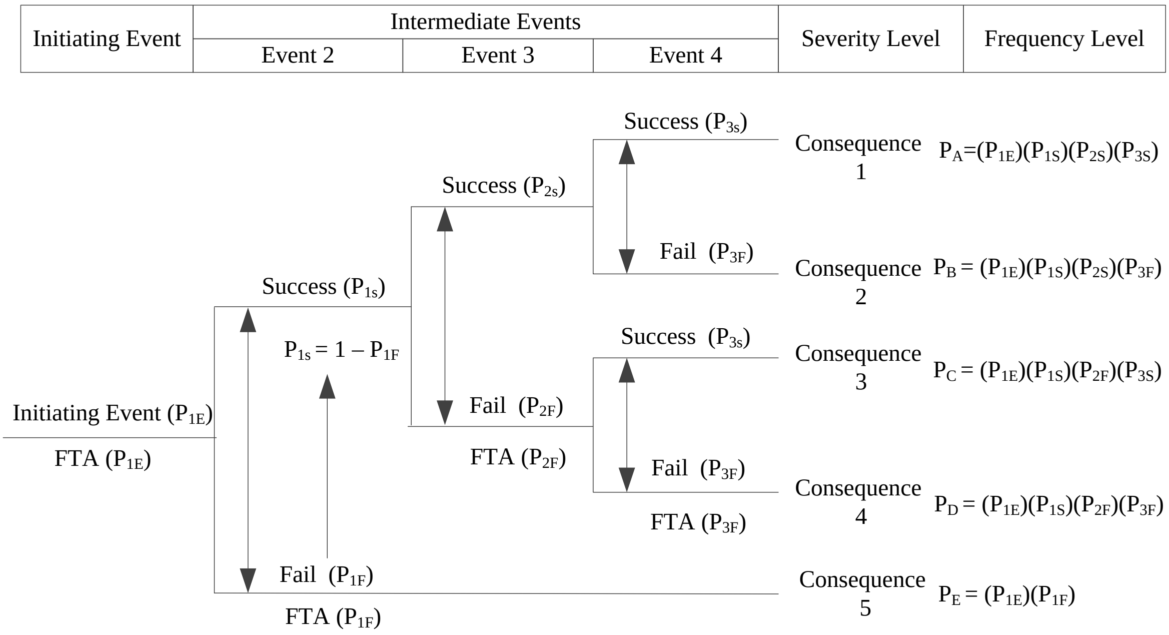


Figure 5.12 Failure Cause-Consequence Quantification Model

5.3.4.1 Qualitative Analysis of Failure Cause Scenarios

A fault tree provides the failure combinations of the components that can cause the top event. The fault tree provides one mechanism that leads the top event. Therefore, the cut set analysis of a fault tree reveals the critical and/or weak links of the components in a system design by identifying safety related to components cut sets with high probability, and where intended safety or redundancy features have been bypassed. The cut set analysis is conducted for the determination of minimal cut sets, which are determined by the rules of Boolean algebra (Stamatelatos and Caraballo, 2002).

The Boolean algebra rules are very important in rules in order to determine minimal cut sets, which are a pictorial expression of the Boolean algebra relationship. Table 5.6 provides Boolean algebra rules being used in general.

Table 5.6 Boolean algebra Rules

	Mathematical Symbolism	Engineering Symbolism	Designation
1-1	$X \cap Y = Y \cap X$	$X \cdot Y = Y \cdot X$	Commutative Law
1-2	$X \cup Y = Y \cup X$	$X + Y = Y + X$	
2-1	$X \cap (Y \cap Z) = (X \cap Y) \cap Z$	$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z$	Associative Law
2-2	$X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X + (Y + Z) = (X + Y) + Z$	
3-1	$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$	$X \cdot (Y + Z) = X \cdot Y + X \cdot Z$	Distributive Law
3-2	$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X + (Y \cdot Z) = (X + Y) \cdot (X + Z)$	
4-1	$X \cap X = X$	$X \cdot X = X$	Idempotent Law
4-2	$X \cup X = X$	$X + X = X$	
5-1	$X \cap (X \cup Y) = X$	$X \cdot (X + Y) = X$	Absorption Law
5-2	$X \cup (X \cap Y) = X$	$X + (X \cdot Y) = X$	
6-1	$X \cap X' = \phi$	$X \cdot X' = \phi$	Complementation
6-2	$X \cup X' = \psi = I^*$	$X + X' = \psi = I^*$	
6-3	$(X')' = X$	$(X')' = X$	
7-1	$(X \cap Y)' = X' \cup Y'$	$(X \cdot Y)' = X' + Y'$	De Morgan's Law
7-2	$(X \cup Y)' = X' \cap Y'$	$(X + Y)' = X' \cdot Y'$	

A fault tree builds a top event by one or more minimal cut sets (MCSs). One basic event, MCS, means a single point failure that will lead to the top event. The two basic events, MCSs, represent the double point failures that together will result in the top event to occur. For an *n*-basic event, MCSs, the top event will be caused when all *n*-basic events in the cut sets are failed (Stamatelatos and Caraballo, 2002).

Therefore, the basic events, MCSs, for the top event can be expressed as:

$$T = M_1 + M_2 + \cdots M_k \tag{5.1}$$

Where,

T = top event;

M_n= MCSs.

Each MCS is comprised of a combination of specific events. Therefore, the general n-basic event MCSs can be expressed as follow:

$$M_n = X_1 + X_2 \cdot \cdots \cdot X_n \tag{5.2}$$

Where,

X_1, X_2… X_n = basic events on the fault tree.

Therefore, Equation 5.1 can be replaced by basic events as Equation 5.3:

$$T = X_1 + X_2 + X_3 + \cdots \cdot X_n \tag{5.3}$$

Equation 5.4 is an example which expresses a top event:

$$T = X_1 + X_2 \cdot X_3 \tag{5.4}$$

Where,

X_1, X_2 and X_3 are basic event failures.

The top event (T) has a one-basic event MCS (X_1) and a two-basic event MCSs ($X_2 \cdot X_3$).

To determine the MCSs of a fault tree, the fault tree is converted into the equivalent Boolean algebra equations. A variety of algorithms exists to translate the Boolean algebra equations into cut sets. The top-down and bottom-up substitution method are the general application methods. The methods are straightforward and they involve substituting and expanding the Boolean algebra expressions. Figure 5.13 is an example fault tree to show the equivalent Boolean algebra equations (Stamatelatos and Caraballo, 2002).

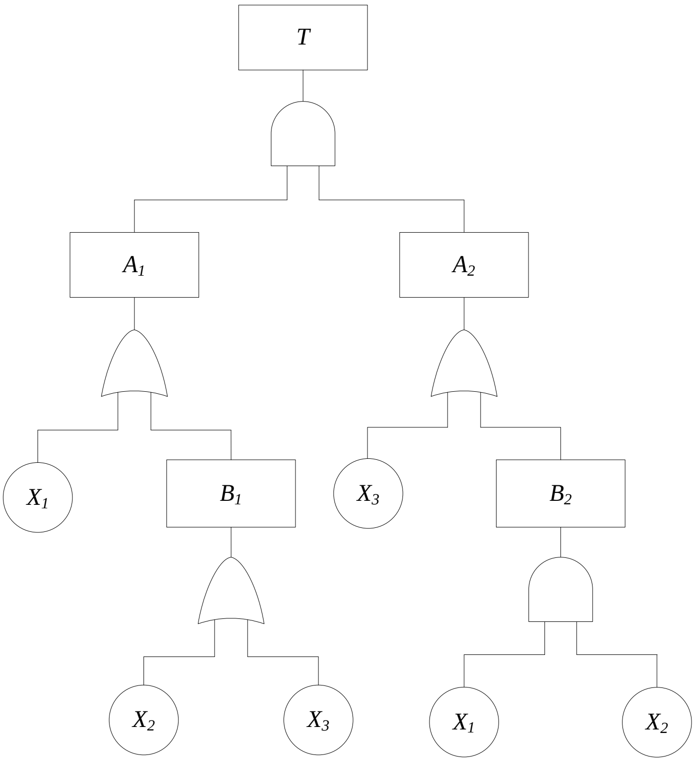


Figure 5.13 An Example of a Fault Tree for the equivalent Boolean algebra

The fault tree shown in Figure 5.13 can be expressed as follows:

$$T = A_1 \cdot A_2 \tag{5.5}$$

$$A_1 = X_1 + B_1 \tag{5.6}$$

$$B_1 = X_2 + X_3 \tag{5.7}$$

$$A_2 = X_3 + B_2 \tag{5.8}$$

$$B_2 = X_1 \cdot X_2 \tag{5.9}$$

❖ Top-down Substitution Method

The first presents the top-down method. Equation 5.5 is replaced by Equations 5.6 and 5.8, and then it is arranged by the absorption law as shown in Equation 5.10:

$$T = (X_1 + B_1) \cdot (X_3 + B_2)$$

$$= (X_1 \cdot X_3) + (B_1 \cdot X_3) + (B_2 \cdot X_1) + (B_1 \cdot B_2) \tag{5.10}$$

Then, B_1 of Equation 5.10 is replaced by Equation 5.7 as below:

$$T = X_1 \cdot X_3 + (X_2 + X_3) \cdot X_3 + B_2 \cdot X_1 + (X_2 + X_3) \cdot B_2$$

$$= X_1 \cdot X_3 + X_2 \cdot X_3 + X_3 \cdot X_3 + B_2 \cdot X_1 + B_2 \cdot X_2 + B_2 \cdot X_3 \tag{5.11}$$

By the idempotent law for the equation given below:

$$X_1 \cdot X_3 + X_2 \cdot X_3 + X_3 + B_2 \cdot X_3 = X_3$$

Thus, Equation 5.11 is simplified as shown below:

$$T = X_3 + B_2 \cdot X_1 + B_2 \cdot X_2 \tag{5.12}$$

B_2 of Equation 5.12 is replaced by Equation 5.9 and then the law of absorption is applied twice, as shown below:

$$T = X_3 + (X_1 \cdot X_2) \cdot X_1 + (X_1 \cdot X_2) \cdot X_2 \tag{5.13}$$

$$(X_1 \cdot X_2) \cdot X_1 = X_1 \cdot X_2$$

Thus, Equation 5.13 is:

$$T = X_3 + (X_1 \cdot X_2) + (X_1 \cdot X_2) \tag{5.14}$$

Then, by the absorption law:

$$(X_1 \cdot X_2) + (X_1 \cdot X_2) = X_1 \cdot X_2$$

Finally, Equation 5.5 can be expressed by minimal cut sets as Equation 5.15:

$$T = X_1 \cdot X_2 + X_3 \tag{5.15}$$

The MCSs of the top event thus consists of one single event MCS (X_3) and one double event MCSs ($X_1 \cdot X_2$). Equation 5.15 can be represented by Figure 5.14.

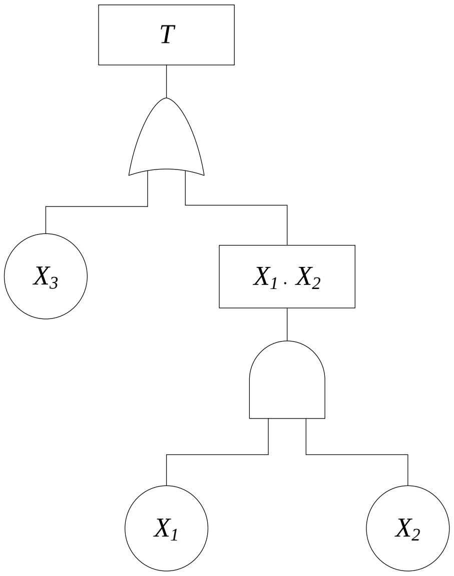


Figure 5.14 Equivalent Fault Tree Simplified from Figure 5.13

- Bottom-up Substitution Method

Bottom-up substitution method for Figure 5.13 follows the procedure as described below. For Equations 5.5 to 5.9, firstly, A$_1$ and A$_2$ are replaced by Equations 5.7 and 5.9 that are made up by only basic events as shown below:

$$A_1 = X_1 + X_2 + X_3 \tag{5.16}$$

$$A_2 = X_3 + X_1 \cdot X_2 \tag{5.17}$$

Then, Equation 5.5 is replaced by Equation 5.6 and 5.8 and the top event can be expressed as shown below:

$$T = (X_1 + X_2 + X_3) \cdot (X_3 + X_1 \cdot X_2) \tag{5.18}$$

Finally, using the absorption law, Equation 5.18 is simplified as Equation 5.19:

$$T = X_1 \cdot X_3 + X_1 \cdot X_1 \cdot X_2 + X_2 \cdot X_3 + X_2 \cdot X_1 \cdot X_2 + X_3 \cdot X_3 + X_3 \cdot X_1 \cdot X_2$$

$$= X_1 \cdot X_3 + X_1 \cdot X_2 + X_2 \cdot X_3 + X_1 \cdot X_2 + X_3 + X_1 \cdot X_2 \cdot X_3$$

$$= (X_1 \cdot X_3 + X_2 \cdot X_3) + (X_1 \cdot X_2 + X_3) + (X_1 \cdot X_2 + X_1 \cdot X_2 \cdot X_3)$$

$$= (X_1 \cdot X_2 + X_3) + (X_1 \cdot X_2 + X_3) + (X_1 \cdot X_2 + X_3)$$

$$= X_1 \cdot X_2 + X_3 \quad (5.19)$$

It is confirmed that Equation 5.15 is equal to Equation 5.19. Therefore, any of these two methods can be used to get the same minimal cut sets.

5.3.4.2 Quantitative Analysis of Failure Cause Scenarios

A failure cause scenario model can be quantified by the probability law or failure rate. These quantifying methods are described below:

(1) Quantification by Probability Law

After the minimal cut sets of a fault tree are determined, the probability of the top event can be evaluated. The basic concepts of the probability laws are applied to the logic gates of FTA. Two basic laws of probability are represented for 'OR' and 'AND' gate:

- <u>OR gate</u>

The probability expression of OR gate for the top event is given by Equation 5.20:

$$P(T) = P(a) + P(b) - P(a \cdot b) \quad (5.20)$$

If a and b are statistically independent events and “$P(a \cdot b)$”is very small, then the above Equation 5.20 can be approximated as Equation 5.21:

$$P(T) \cong P(a) + P(b) \quad (5.21)$$

In the case of *n* number of inputs OR gate, the Equation 5.21 may be generalised by Equation 5.22:

$$P(a + b + c + \cdots) \cong P(a) + P(b) + P(c) + \cdots \qquad (5.22)$$

- AND gate

The probability expression of AND gate for the top event is given by Equation 5.23:

$$P(ab) = P(a) \cdot P(b) \qquad (5.23)$$

For AND gate of *n* input, the above Equation 5.23 can be generalised as Equation 5.24:

$$P(a \cdot b \cdot c \cdot \cdots) \cong P(a) \cdot P(b) \cdot P(c) \cdots \qquad (5.24)$$

(2) Quantification by failure Rate

- OR gate

Logically the OR gate corresponds to a series system, the reliability of which is evaluated by the following Equation 5.25:

$$R_s(t) = \prod_{i=1}^{n} R_i\ (t) \qquad (5.25)$$

Where,

R_i = the reliability of the *i*th component;

R_s = the series system reliability and;

n = the number of components.

The failure rate, F (t), is a probability complementary to reliability, as shown below:

$$F(t) = 1 - R(t) \qquad (5.26)$$

Therefore, the failure rate of a series system can be represented by Equation 5.27:

$$F_s(t) = 1 - \prod_{i=1}^{n}(1 - F_i\ (t)) \tag{5.27}$$

Where,

F_i = the failure rate of the ith component;

F_s = the series system failure rate, and;

n = the number of components.

- <u>AND gate</u>

The AND gate corresponds to a logically connected parallel system. Reliability of the parallel system is given by the following equation:

$$R_p(t) = 1 - \prod_{i=1}^{n}(1 - R_i(t)) \tag{5.28}$$

Where,

R_p = the parallel system reliability;

n = the number of components, and;

R_i = the ith component reliability.

On the other hand, the failure rate of the parallel system is given by the following equation:

$$F_p(t) = \prod_{i=1}^{n}(F_i(t)) \tag{5.29}$$

Where,

F_i = the failure rate of the ith component;

F_p = the parallel system failure rate, and;

n = the number of components.

Figure 5.12 shows the methods that analyse the probability of failure frequency of each failure event through consequence scenarios developed in previous phases (Ericson, 2005).

5.3.5 Risk Evaluation Phase

The risk evaluation phase is performed to determine the risk level by the combination of the failure severity and its frequency levels through the risk evaluation matrix. The results obtained from this phase will provide important information for the selection of appropriate risk handling and control options. The evaluated results are used to assist the systems engineers or RAMS engineers to design system products and develop maintenance, logistic support and operation schemes. If the risk requires high-risk measures, it has to be controlled to reduce the failure frequency or any possible failure consequences. If the risks were accepted, no further action would be required, but the analysis results provided would need to be recorded for certification (Umar, 2010; BS ISO/IEC 31010, 2008).

5.4 Summary

This chapter has presented railway risk assessment method, based on the combination of FMEA-FTA to support the control of railway RAMS risks that affect the mission and safety of railway service. The hazards, information and data available and systems design phase are important decision-making factors for the selection of railway risk assessment techniques.

This chapter firstly presented railway risk assessment models, based on the definition of railway risk and the application of FMEA-FTA combination. This chapter presented four questions for the definition of railway risk, the construction of risk scenarios and the selection of the risk assessment techniques, and it also provided the method of applying FMEA-FTA combination to the railway risk scenario. This chapter presented two FMEA-FTA based risk assessment models, top-down and bottom-up, that are applicable to the functional and design architecture design phases.

This chapter secondly provided FMEA-FTA based railway risk assessment process that is applicable to all systems design phase to cover all aspects of railway risk assessment, based on the systems engineering process. The process is started with the definition of RAMS design and acceptance criteria. In the risk identification phase, the process proposed the use of ETA and fishbone diagram to identify all possible risks effectively. The ETA can be used for the graphical representation of the failure consequence scenarios and the fishbone diagram can be used for the exact determination of the failure causes and the effective support of a fault tree construction.

The identified railway risks are analysed qualitatively and quantitatively to quantify the frequency and severity of the failure consequences. The qualitative analysis is conducted to determine minimal cut sets, which exactly identifies the causes of a failure consequence, especially, to determine the safety functions and their monitoring functions and the quantitative analysis is performed to quantify the determined minimal cut set by the failure probability or failure rate

In conclusion, railway risk assessment is a core part of RAMS management and systems engineering, providing a thorough understanding and sufficient information for the effective control of railway risks. The proposed risk assessment methods can easily be used in the systems design phase and have a great potential to design the system safety functions. However, the risk assessment process requires the thorough understanding for the railway system functions and failures, its operation conditions, adequate risk data sources and many experiences and knowledge.

Chapter 6

DEVELOPMENT OF PERFORMANCE BASED RAMS SPECIFICATION FOR RAILWAY SYSTEM REQUIREMENTS

6.1 Introduction

Chapters 4 & 5 have discussed the method to establish railway RAMS management and integrate the RAMS management into railway systems engineering. For this objective, a RAMS management systems with risk based RAMS management process was proposed, and a railway systems engineering process and its detailed process activities were established to provide the fundamentals of the policy, functions and activities of the RAMS management. A FMEA-FTA based railway risk assessment method was also presented to focus RAMS management on the assessment and control of railway risks that affect the quality of railway service. These resultant outcomes lay the foundations for development of RAMS specification that provides RAMS design solutions and its acceptance criteria.

Specifying RAMS requirements and operational contexts is a starting point for implementing RAMS management through systems engineering process; it provides a basis for performing RAMS management activities. RAMS specification shall require the systematic and quantitative RAMS requirements and operational strategies to the customers. On the other hand, it also requires the development of technical RAMS design and its acceptance criteria to the supplier. Therefore, developing RAMS specification is an essential activity to both the customer and the supplier to achieve the objective of RAMS management and increase the feasibility of the system design in the operation phase. However, in many railway projects, customers have not provided systematic and quantitative RAMS requirements and operational conditions to the suppliers. The suppliers have also not systematically developed RAMS specification with the customers. In fact, railway projects have just provided RAMS specification without the implementation of RAMS specification process. Thus, railway projects have undergone many difficulties in ensuring that RAMS requirements can be achieved in the system concept design phase and some projects were even failed. Therefore, this chapter presents the method that develops systematic and quantitative RAMS requirements by the customers, and develops technical RAMS design criteria by the suppliers.

This chapter comprises five sections to present the development of railway RAMS specification. Section 6.2 presents a framework to develop RAMS performance specification. A proposed railway RAMS specification process is presented in Section 6.3. This chapter is concluded in Section 6.4 with a brief summary.

6.2 Development of Railway RAMS Performance Specification

6.2.1 Railway RAMS Performance Specification

A railway systems specification shall accurately describe all function and performance requirements required for the establishment of technical design solutions and their acceptance criteria, operational conditions and test provision. It aims at ensuring that all system requirements should be achieved successfully during the system design and operation phases. It also includes the essential internal and external constraints. A railway system performance specification provides the overall design solutions, its acceptance performance criteria and the operational contexts of the system to design; it is also allocated to the subsystems comprising the system to establish the optimal functional architecture. RAMS performance specification shall be conducted in the same way as an integrated part of the systems performance specification to facilitate the system design efforts (BS EN 62347, 2007).

RAMS performance specification is generally implemented for the achievement of the following objectives: (1) to avoid duplication, conflict and inconsistency of the performance related to RAMS management activities that may occur during railway systems engineering is progressed, (2) to analyse and evaluate RAMS requirements and operational behaviours adequately, (3) to negotiate for contract and reference of RAMS performance that may be caused due to the changes in the system engineering policy, methods, and techniques, (4) to support configuration management and (5) to consistently communicate with the customer, especially related to responsibility (Duap, 2001).

6.2.2 Development of Railway RAMS Performance Specification

RAMS performance specifications have been provided from many railway projects, but the principle, method, techniques and process for the development of RAMS performance specification have not been provided from railway industry and other mission and safety critical industrial fields as well. Therefore, this section proposes a framework that can specify RAMS requirements and operational contexts into RAMS design and its acceptance performance criteria as shown in Figure 6.1. The framework provides a foundation for the development of RAMS performance specification of a railway system.

Figure 6.1 describes a proposed framework for the development of RAMS performance specification and it is based on the systems approach, as stated in Chapter 3. The proposed framework consists of five steps under the thorough understanding of the entire railway service objectives: (1) the establishment of railway service objectives, (2) the definition of railway RAMS, (3) the establishment of principle for RAMS performance specification, (4) the establishment of RAMS measures and (5) the development of RAMS performance specification process. The RAMS performance specification process should be consistently applied and implemented in all system design phases.

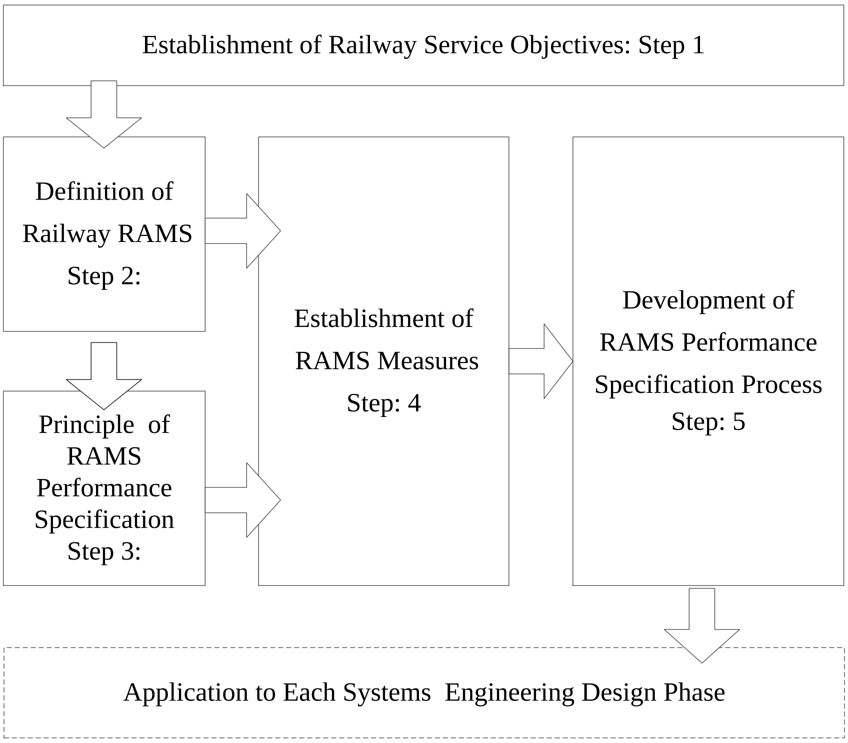

Establishment of Railway Service Objectives: Step 1
Definition of Railway RAMS Step 2:
Principle of RAMS Performance Specification Step 3:
Establishment of RAMS Measures Step: 4
Development of RAMS Performance Specification Process Step: 5
Application to Each Systems Engineering Design Phase

Figure 6.1 Framework for Development of Railway RAMS Performance Specification

Step 1: Establishment of Railway Service Objectives

RAMS performance specification is started with the identification of the overall railway service objectives in the entire railway business aspect and the establishment of the service performance that takes on the railway system to design. The railway service performance shall effectively satisfy the achievement of the overall railway service objectives and it is a basis of railway RAMS performance specification as an input. Therefore, the quantitative definition of the railway service objectives is very important to develop the RAMS design solutions and their acceptance performance criteria.

Step 2: Definition of Railway RAMS

Definition of railway RAMS as a framework, as shown in Figure 6.2, is to provide the RAMS concepts and operational strategies of the system to design and develop. It generally includes railway service objectives, operational RAMS objectives, operational contexts and product RAMS measures as shown in Figure 6.2. However, the RAMS definition can be tailored from the framework of Figure 6.2, depending on railway service objectives and operational strategies. For example, the goal of the railway service is to achieve the level of a defined railway traffic service within the defined time and limited cost safely. The defined time, limited cost, safety and the defined service level are important factors to define railway RAMS and its performance level. If the defined time means the arrival time at the terminal station, it can only define reliability. However, if the defined time means both readiness at the departure station and the arrival time at the terminal station, it can define availability, including both reliability and maintainability. The planned cost greatly affects the performance level of RAMS measures as shown in Figure 6.2 (BS EN 50126-1, 1999).

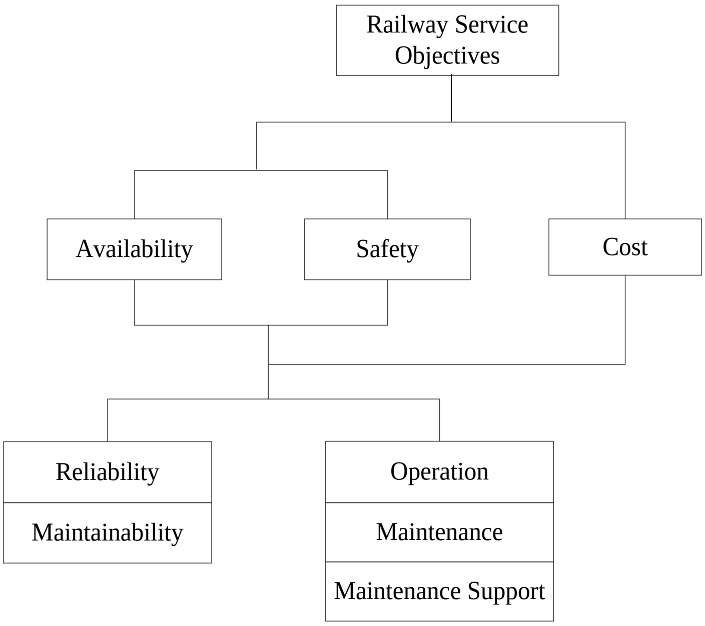


Figure 6.2 Definition of Railway RAMS Elements

Step 3: Establishment of RAMS Performance Specification Principle

The railway RAMS definition of Figure 6.2 provides the basis for RAMS performance specification. Figure 6.3 presents a proposed principle that specifies RAMS design solutions and their acceptance performance criteria, which is modified from Figure 6.2. The RAMS performance specification is implemented by three steps and their interaction as shown in Figure 6.3 (Green, 2001; Daup, 2001).

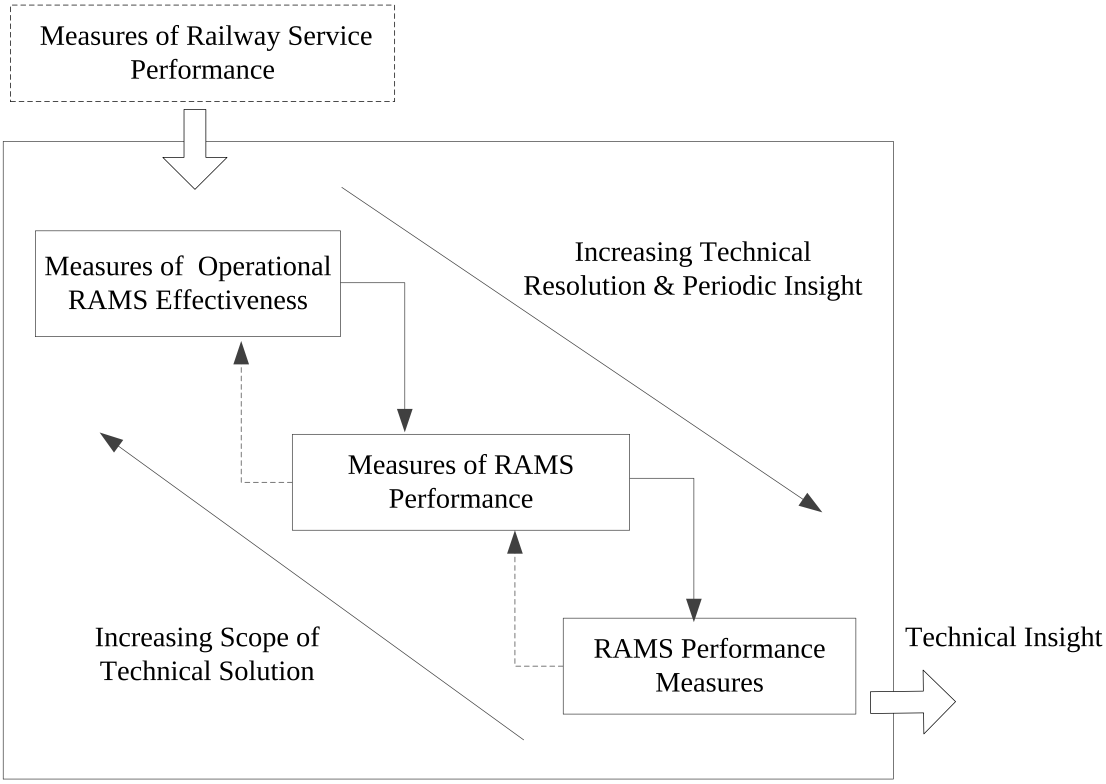

Measures of Railway Service Performance
Increasing Technical Resolution & Periodic Insight
Measures of Operational RAMS Effectiveness
Measures of RAMS Performance
Increasing Scope of Technical Solution
RAMS Performance Measures
Technical Insight

Figure 6.3 Principle of Railway RAMS Performance Specification

(1) Establishment of Measures of Railway Service Performance

The objective of RAMS performance specification is to effectively contribute to the successful achievement of the overall railway service objectives in the rail traffic business aspect. Therefore, RAMS performance specification is started with identifying the overall railway service objectives and establishing the railway service performance which undertakes the system to design and its measures. The railway service performance and measures become an input of RAMS performance specification as shown in Figure 6.3.

(2) Definition of Operational RAMS Effectiveness

Operational RAMS effectiveness is the measure that is designed to correspond to the achievement of railway operational objectives, which are closely related to the achievement of the railway service objectives. It focuses on how well the railway service objectives are achieved, and how well the system being designed is integrated successfully into the operational conditions. In general, there are many measures of operational RAMS effectiveness, but the availability, safety and cost can be defined as the measures of operational RAMS effectiveness as described in Figure 6.2.

(3) Definition of Measures of RAMS Performance

Measures of RAMS performance are the quantitative measures that define the functional or design architectures of a railway system. These performance and measures are generally defined from the specified operational conditions and they shall be considered for the successful achievement of the operational RAMS effectiveness, but they are not directly measured. The assessment of the operational conditions is the basis for the determination of the quantitative RAMS performance (Kapurch, 2010).

(4) Determination of RAMS Performance Measures

RAMS performance measures are directly derived from the measures of operational RAMS effectiveness and RAMS design performance; they become the RAMS design solutions and acceptance performance criteria. The RAMS performance measures are used for a periodic review and control of the acceptance performance criteria for the system design efforts and they are used in the system design process to assess the achievement of the system requirements, monitor the achievement of them and identify risks.

In RAMS management, RAMS performance measures are generally used for the followings (Kapurch, 2010):

- To predict RAMS performance measures to be achieved;
- To identify the difference between the actual RAMS performance measures and planned ones;
- To support the assessment of measures of RAMS performance, and;
- To assess RAMS performance measures for the changes of the system design.

Step 4: Determination of RAMS Measures

The four steps determine the RAMS measures needed to variously assess the measures of the effectiveness of the operational RAMS and the RAMS design performance. Figure 6.4 describes a framework of basic RAMS measures produced in the RAMS specification process phase. However, the customer or supplier may require various RAMS measures to evaluate the performance of RAMS design effectively as if needed as provided in Tables 6.1, 6.2 and 6.3.

Step 5: Development of Railway RAMS Performance Specification Process

The final step is to develop the RAMS specification process to resolve the RAMS performance issues, based on the systems performance specification process. The detailed process activities of the RAMS performance specification process will be presented in Section 6.3.

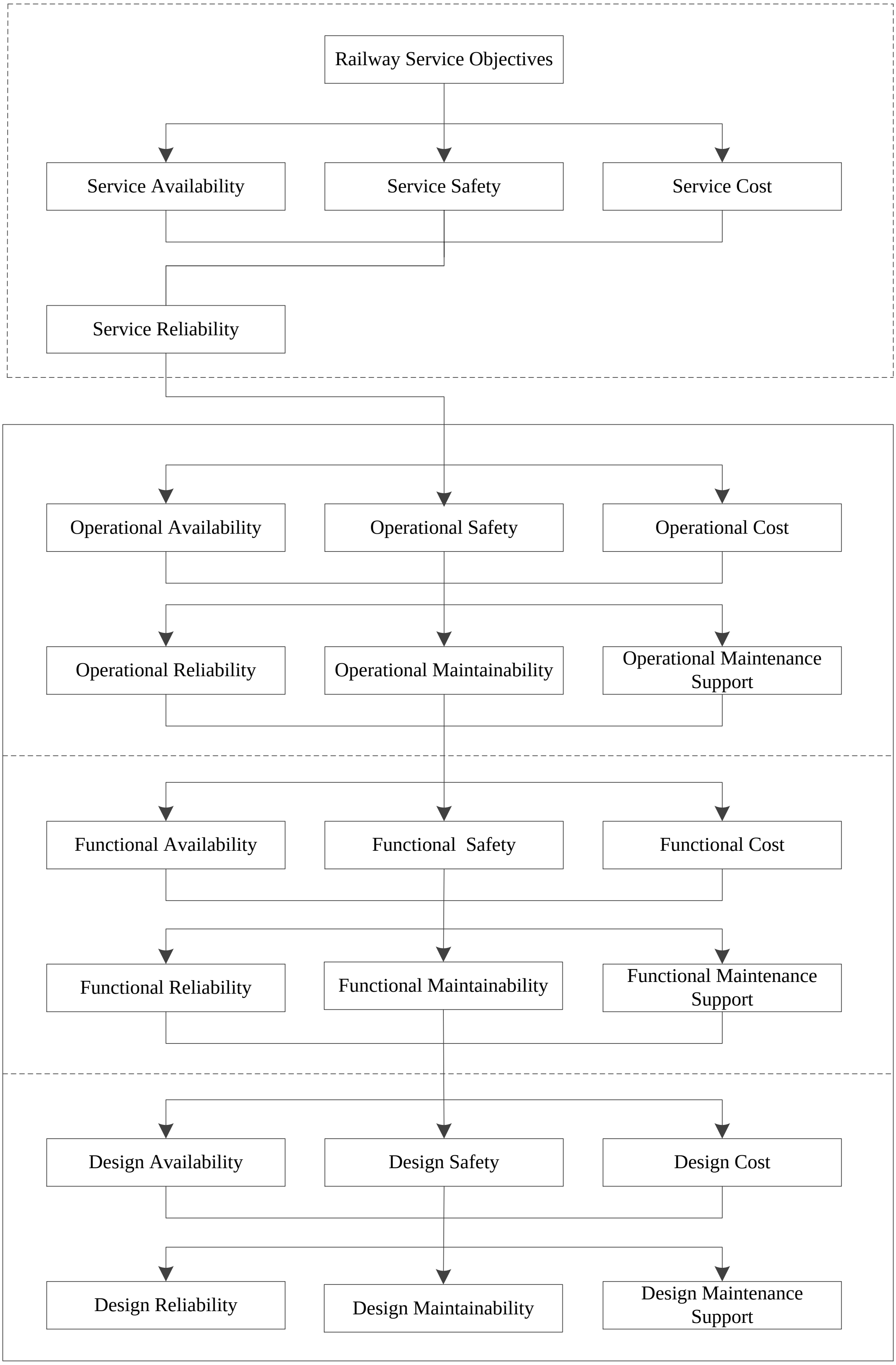


Figure 6.4 Framework of Proposed Railway RAMS Measures

Table 6.1 Examples of Availability and Safety Measures

Availability		Safety	
Measure	Symbol	Measure	Symbol
Availability Inherent Achieved Operational	A A_i A_a A_o	Mean Time Between Hazardous Failure	MTBF (*H*)
Fleet Availability	FA	Mean Time Between 'Safety System Failure'	MTBSF
Schedule Adherence	SA	Hazard Rate	H(*t*)
		Safety Related Failure Probability	Fs(*t*)
		Probability of Safe Functionality	Ss(*t*)
		Time to Return to Safety	TTRS

Table 6.2 Examples of Reliability and Maintainability Measures

Reliability		Maintainability	
Measure	Symbol	Measure	Symbol
Failure Rate	λ	Mean Down Time	MDT
Mean Up Time	MUT	Mean Time/Distance Between Maintenance	MTBM/MDBM
Mean Time to Failure Mean Distance To Failure	MTTF MDTF	MTBM/MDBM, Corrective or Preventive	$MTBM_{c/P}$ $MDBM_{c/P}$
Mean Time Between Failure Mean Time Between Failure	MTBF MDBF	Mean Time To Maintenance	MTTM
Failure Probability	F(*t*)	MTTM, Corrective or Preventive	$MTTM_{c/p}$
Reliability (Success Probability)	R(*t*)	Mean Time To Repair	MTTR

Table 6.3 Examples of Maintenance Support Measures

Measure	Symbol	Measure	Symbol
Operation and Maintenance Cost	O&MC	Maintenance Man Hour	MMH
Maintenance Cost	MC	Logistic & Administrative Delay	LAD
Fault Correction Time		Repair Time	
Maintenance support Performance		Employees for Replacement	EFR

6.3 Development of Railway RAMS Performance Specification Process

This section presents a process which is applicable to all the different design phases to define the performance value of the RAMS design and its acceptance criteria. Figure 6.5 describes a proposed railway RAMS performance specification process and its key process activities. The process is based on Figures 6.1 to 6.4 and it consists of an input and three performance definition phases: i.e., (1) service RAMS definition phase, (2) operational RAMS definition phase, (3) functional RAMS definition phase and (4) design RAMS definition phase.

The specification process should cover all aspects that quantitatively define RAMS design solutions and their acceptance criteria through the various design steps in order to reach a rational decision making with regards to the optimal and balanced RAMS performance design and its acceptance criteria. The specification process includes sufficient activities for the successful achievement of all functional requirements to demonstrate the RAMS design performance criteria required in the operational conditions, and demonstrate that all potential hazards that are included in the functions are defined, assessed and appropriately controlled to bring the acceptance level of risks to ALARP[20].

Each phase of the process includes the specific activities and techniques to achieve its specific design objectives. Thus, each process phase focuses on the specific activities and techniques, for example, the allocation of railway service performance targets, the assessment of the operational behaviours, RAMS performance trade-off/control, the allocation of RAMS performance requirements into the lower systems and the establishment of RAMS design verification and acceptance criteria. The operational RAMS performance definition phase is the basis of the RAMS performance specification process activities as shown in Figure 6.5.

[20] As Low As Reasonably Practicably

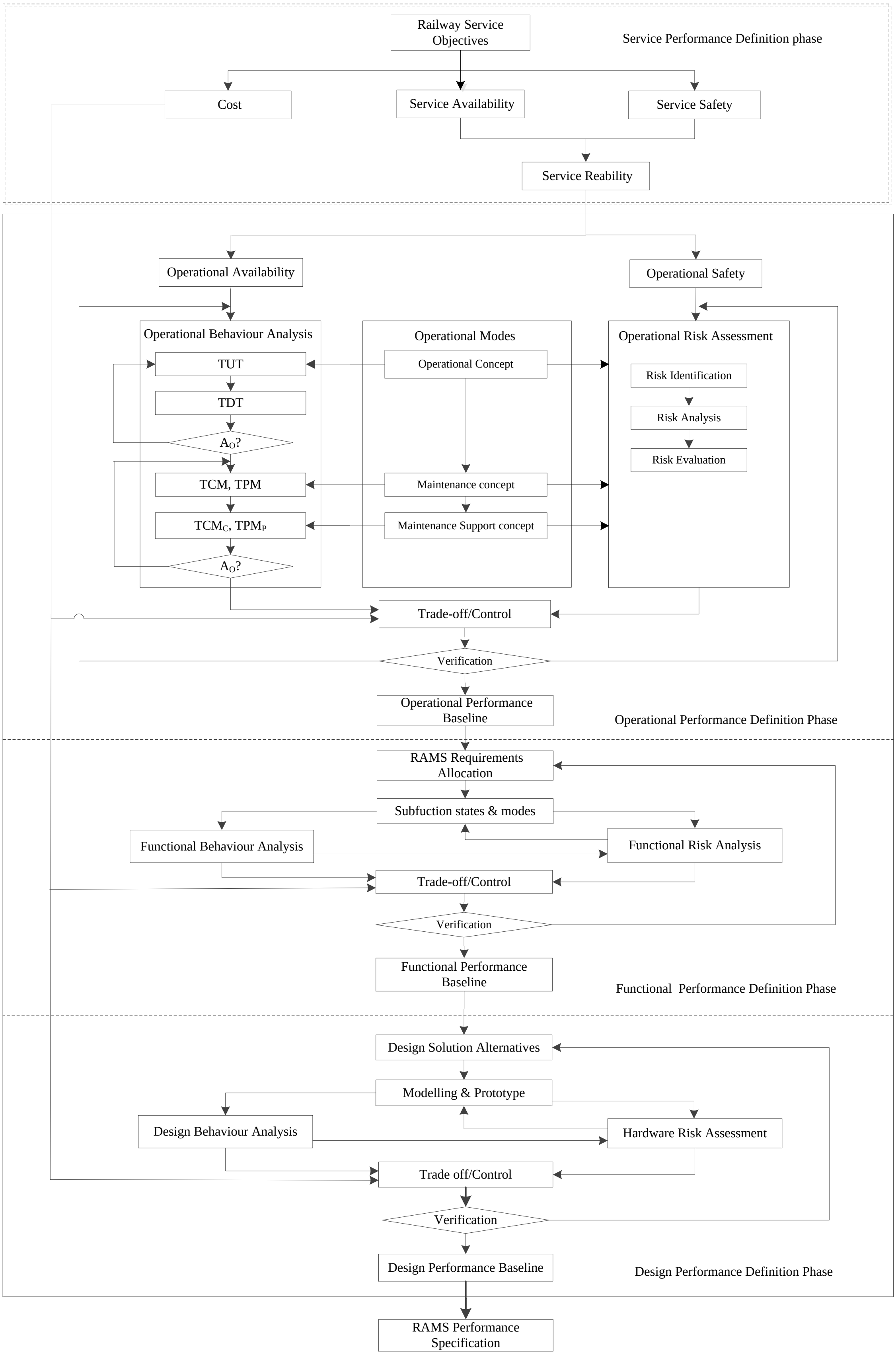

Railway Service Objectives
Service Performance Definition phase
Cost
Service Availability
Service Safety
Service Reability
Operational Availability
Operational Safety
Operational Behaviour Analysis
TUT
TDT
A_O?
TCM, TPM
TCM_C, TPM_P
A_O?
Operational Modes
Operational Concept
Maintenance concept
Maintenance Support concept
Operational Risk Assessment
Risk Identification
Risk Analysis
Risk Evaluation
Trade-off/Control
Verification
Operational Performance Baseline
Operational Performance Definition Phase
RAMS Requirements Allocation
Subfuction states & modes
Functional Behaviour Analysis
Functional Risk Analysis
Trade-off/Control
Verification
Functional Performance Baseline
Functional Performance Definition Phase
Design Solution Alternatives
Modelling & Prototype
Design Behaviour Analysis
Hardware Risk Assessment
Trade off/Control
Verification
Design Performance Baseline
Design Performance Definition Phase
RAMS Performance Specification

Figure 6.5 Proposed Railway RAMS Performance Specification Process

6.3.1 Service RAMS Performance Definition Phase

This phase provides an input as a basis for the RAMS performance specification process. It is a process which identifies the overall railway service objectives, included measures and their performance targets, and determines the service RAMS performance targets that conduct the system to design and develop. The railway service RAMS performance targets are determined by the allocation techniques as stated in Chapter 3. In general, railway service RAMS measures are defined by service safety and availability as measures of service effectiveness and service reliability as technical RAMS performance measure as described in Figure 6.5. There are many allocation techniques applicable as described in Chapter 3, but the ARINIC allocation technique using failure rate can be used effectively in this phase.

6.3.2 Operational RAMS Performance Definition Phase

This phase is a process which determines the measures of operational RAMS effectiveness[21] through the railway service objectives and establishes the performance of operational RAMS effectiveness through the assessment of operational behaviours for the operational scenarios. The overall activities of this process phase provide a basis for other process activity as shown in Figure 6.5. The process phase consists of four activities: i.e., (1) the determination of operational RAMS effectiveness targets, (2) the assessment of operational behaviours, (3) RAMS performance trade-off/control and (4) RAMS performance verification as shown in Figure 6.5. The process phase starts with the determination of operational (or system) RAMS effectiveness.

[21] Operational RAMS effectiveness = RAMS effectiveness of the system level to develop

6.3.2.1 Determination of Operational RAMS Effectiveness

Figure 6.5 provides operational availability and safety as measures of operational effectiveness. In general, the availability performance target is defined as the probabilistic value; the safety performance target is defined as the deterministic value as mentioned in Chapter 5 (Ebeling, 2010; Tray et al., 1997).

(1) Determination of Operational Availability Target

Operational availability performance target shall satisfy the service availability and operational cost assigned as described in Equation 6.1. Thus, the operational availability is determined by the operational cost and service availability performance targets. Equation 6.1 can be generally used for determining operational availability performance (MIL-HDBK-388B, 1984; Carlier et al., 1996):

$$A_s = \sum_{x}^{n} \binom{n}{x} A_0^x (1 - A_0)^{n-x} \qquad (6.1)$$

Where,

A_s= Service availability performance target;

A_0 = Operational availability performance target to determine;

x = Minimum cost (or systems) needed for the achievement of operational RAMS requirements, and;

n = Maximum cost (or systems) to be determined for the achievement of operational RAMS requirements.

(2) Determination of Operational Safety Target

Operational safety performance target is determined by the external and internal constraints, for example, regulations, standards, laws etc. and the performance is established through risk assessment that may be included in the rail traffic service conditions as shown in Figure 6.5. The operational risk assessment is performed by PHA as stated in Chapter 3 and the performance target is given as deterministic values such as the level of failure severity and frequency as stated in Chapter 5.

6.3.2.2 Assessment of Operational behaviour

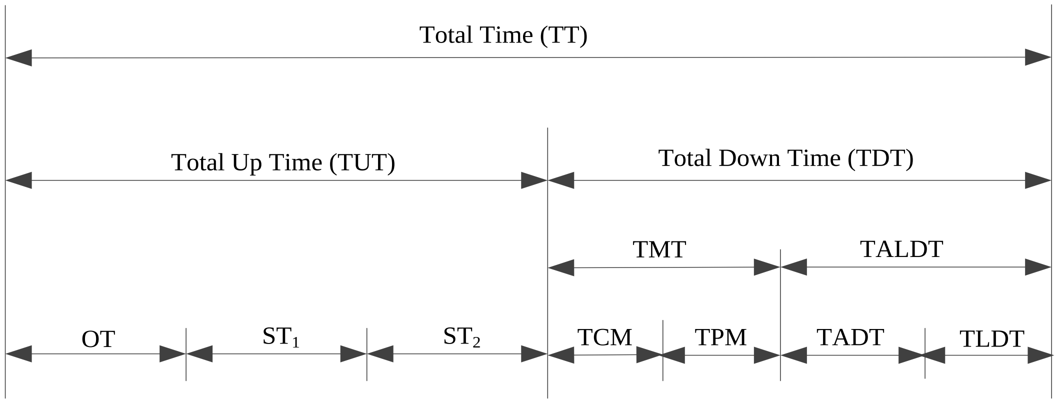
The performance value of operational RAMS measures is established through the assessment of the operational behaviours for the operational scenarios. The operational behaviours are assessed for the operational risks and timeline, as shown in Figure 6.5. The operational assessment is conducted by four steps as below:

Step 1: Establishment of Operational Behaviours

The first step of the operational behaviour assessment commences with the establishment of operational modes to assess. The operational modes related to RAMS performance specification can include operation, maintenance and maintenance support. In most railway projects, maintenance support has not been included in the RAMS performance specification, but the maintenance support performance has great influence on the RAMS design performance. Therefore, maintenance support performance shall be considered in the RAMS performance specification (Krri, 2007).

Step 2: Timeline Definition of Operational Behaviours

Defining the timeline of operational behaviours is essential for the assessment of operational RAMS effectiveness for the operational behaviours of the system to design and develop. Figure 6.6 describes the defined timeline for operational behaviours, which are classified by total up time and down time. The total up time consists of operating time and standby time. The total down time includes maintenance and maintenance support time (Stapelberg, 2009).



TMT	Total Maintenance Time
TALDT	Total Administrative Logistic Delay Time
OT	Operation Time
ST$_1$	Standby Time in operation (system warm)
ST$_2$	Standby Time after operation (system cold)
TCM	Total Corrective Maintenance Time
TPM	Total Preventive Maintenance Time
TADT	Total Administrative Delay Time
TLDT	Total Logistic Support Delay Time

Figure 6.6 Timeline Definition of Operational Behaviour

Step 3: Definition of Mathematical RAMS Measures

The next step is to define the mathematical models of the RAMS measures to evaluate the RAMS performance required in the operational behaviours.

(1) Availability Measure Models

Availability is classified as inherent availability, achieved availability and operational availability.

Equations 6.2 to 6.4 define availability mathematical models, as shown below:

- Inherent Availability (A_i):

$$A_i = \frac{TUT}{TUT + TCM} \tag{6.2}$$

- Achieved Availability (A_a):

$$A_a = \frac{TUT}{TUT + TCM + TPM} \tag{6.3}$$

- Operational Availability (A_o):

$$A_o = \frac{TUT}{TUT + TDT} \tag{6.4}$$

(2) Reliability Measure Model

Reliability is defined as "the failure frequency that has occurred over total operating time, namely, mean time (or distance) between failures (MTBF)". Accordingly, the MTBF can be obtained by the definition between TALDT and ALDT, as shown in Equation 6.5 (Kim et al., 2008):

$$TALDT = \frac{OT}{MTBF} \times ALDT \tag{6.5}$$

Firstly, apply Equation 6.5 to Equation 6.4:

$$A_o = \frac{TUT}{TUT + TDT} = \frac{TT - TMT - TALDT}{TT}$$

$$= \frac{TT - TMT - \frac{OT}{MTBF} \times ALDT}{TT} \tag{6.6}$$

Then, Equation 6.6 can be arranged again as reliability measure 'MTBF' as shown in Equation 6.7:

$$MTBF = \frac{OT \times ALDT}{(1 - A_o)TT - TMT} \tag{6.7}$$

(3) Maintainability Measure Model

Maintainability is defined by the preventive and corrective maintenance time, but the corrective maintenance model is generally defined because the preventive maintenance time can be simply obtained by the customer's maintenance strategy. The ratio of maintenance time for the total operational time, or maintenance rate, can be defined if needed. Equations 6.8 and 6.9 describe the mathematical model of corrective maintenance time and maintenance rate:

- Mean Corrective Maintenance Time (*MTTR*):

$$MTTR = \frac{TCM\ \times OT}{MTBF} \tag{6.8}$$

- Maintenance Rate (*MR*):

$$MR = \frac{TCM + TPM}{OT} \tag{6.9}$$

Step 4: Operational Risk Assessment

As mentioned above, operational railway risk assessment generally applies preliminary hazard analysis (PHA) to provide an initial overview of a railway risks such as the identification of all possible potential hazards, their causal factors, effects, level of risk and control of the risk as stated in Chapter 3. The methods to railway risk assessment were discussed in Chapters 4 and 5 in detail.

6.3.2.3 RAMS Performance Control

The operational RAMS performance assessed through the RAMS performance specification process can conduct trade-off in the availability, safety and cost aspects if needed to prevent the conflict of the RAMS performance as shown in Figure 6.5. The trade-off method and procedure were discussed in Chapters 4 and 5. Therefore, this section provides two examples for trade-off of RAMS performance assessed as described in Figures 6.7 and 6.8. Figure 6.7 is an example of the trade-off method with regards to the technical aspect based on availability performance. Figure 6.8 describes an example of the trade-off method with regards to the cost and safety aspects.

Step 1: Availability Based RAMS Performance Trade-off

Figure 6.7 shows an example of a reliability and maintainability performance trade-off. This trade off can be generally implemented to control the maintainability and reliability performance by the availability performance target. Figure 6.7 shows the trade-off range of reliability performance and maintainability performance based on availability target. The shaded area of Figure 6.7 shows the range that can perform the trade-off for minimum reliability performance measure (MTBF: 400 hours) and maximum maintainability performance measure (MTTR: 4 hours) to satisfy the availability performance target, 99% (MIL-HDBK-388B, 1984).

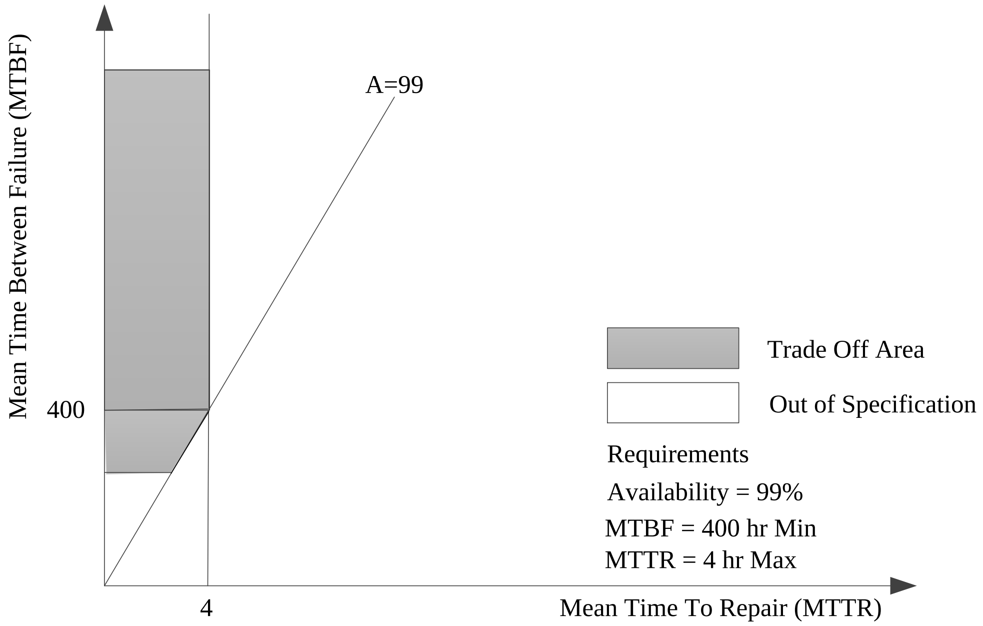


Figure 6.7 An Example of RAMS Trade-off in Availability Aspect

Step 2: Cost and Safety Based RAMS Performance Trade-off

Figure 6.8 shows an example of trade-off of reliability and maintainability performance with regards to the cost and safety aspect. The safety performance target depends on the planned cost as shown in Figure 6.8. In the figure, horizontal axis 1 represents maintainability (preventive maintenance interval); horizontal axis 2 is the availability based reliability performance (minimum reliability) needs for the achievement of operational availability, and horizontal axis 3 is the safety reliability performance which is required for the achievement of operational safety. Curve 4 explains the changes of reliability performance compared with maintainability performance, and curve 5 shows the change of cost required for maintainability performance. Area “A” is a high cost area because many frequencies of maintenance are required by low reliability performance. Area “C” is also of a high cost and over the reliability performance area, in spite of high maintenance interval. However, area “B” is the area of the lowest cost and the reliability performance is satisfied for safety reliability performance limitation. Therefore, RAMS design performance will be determined in the area B.

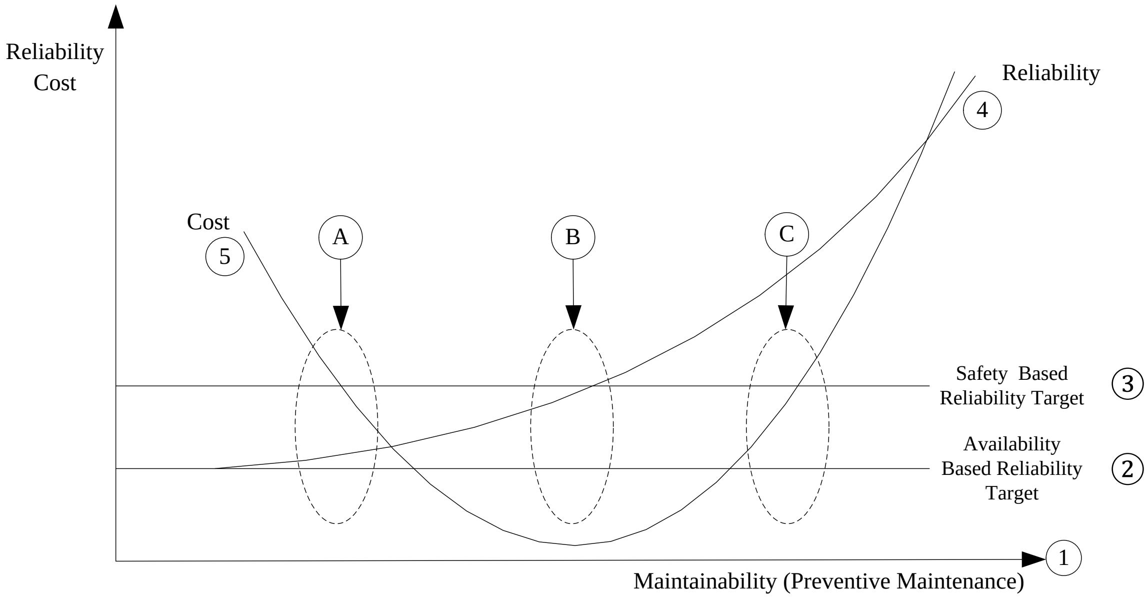


Figure 6.8 An Example of RAMS Trade-off in Cost Aspect

Step 3: RAMS Performance Management

The RAMS performance characteristics which were established by the trade-off are applied to the lower system design. Figure 3.19 of Chapter describes RAMS design methods.

6.3.2.4 RAMS Performance Verification

The RAMS design performance established by RAMS control shall be verified to assure the achievement of operational RAMS requirements through the selected verification method. The detailed verification method will be described in Section 6.3.4.

6.3.3 Functional RAMS Performance Definition Phase

This phase is a process that defines RAMS design performance and its acceptance criteria for the specific functions[22] comprising a system. It is started with the allocation of the operational RAMS performance to the subsystems. The allocated RAMS performance is established through the functional timeline analysis and the risk analysis of functional state and modes, as shown in Figure 6.5. Therefore, the allocation of RAMS performance is a basis and key process activity of this phase (BS ISO/IEC 26702, 2008).

The allocation of the operational RAMS performance is an essential design activity that establishes the optimal and balanced functional architectures. In general, it is generally dependent on the complexity of the sub-functions to be allocated, based on the experience of similar system. The performance allocation is considered for various factors if possible, such as complexity, criticality, operational profile and environmental conditions. However, if the information and data available is very limited, various approaches, such as engineering judgement or expert opinion, should be considered. Therefore, this section discusses the methods that allocate the operational RAMS performance in terms of the engineering judgement of systems engineering team compared with a selected similar system. The RAMS performance allocation is conducted for reliability and maintainability in this phase (MIL-HDBK-388B, 1984; Nicholls, 2005).

6.3.3.1 Reliability Performance Allocation

Several reliability allocation methods were reviewed in Chapter 3. The allocation methods can be applied by the information and data available, but at the system concept stage, the information and data may be very limited. Thus, this section presents a reliability performance

[22] Specific functions = subsystems

allocation method using the engineering judgement by a comparative system that is the most similar to the system to design. The performance of the selected comparative system and the engineers' knowledge and experience for system are key factors in this allocation method. Table 6.4 describes the evaluation factors and their possible evaluation range (Eo et al., 2010).

Table 6.4 Reliability Performance Allocation Factors

Evaluation Factors	Evaluation Factor Description	Range & Score
System Complexity	System complexity means the probable number of parts or components comprising the subsystem.	0.8 – 1.2
System Criticality (state-of-the-art)	System criticality means the state of present engineering progress.	0.8 - 1.2
Operating Time	Operation time means the real operating time for entire mission time.	0.8 – 1.2
Operational Environment	Operational environment means the severity of the operating real environment.	0.8 – 1.2

As described in Table 6.4, the evaluation factor for the RAMS allocation should be considered in the operational and technical aspect of the system to evaluate. Therefore, the operational factor is selected for the operating time and environmental severity of the subsystem assigned and the technical factor is selected for the complexity and criticality of the subsystem. The range of the evaluation factors are classified within the range of ± 20 %: + 20 % ranges for improvement and upgrade or - 20 % for down-grade, to reduce the range of the subjective judgements and to use the most similar system possible.

The evaluation of the allocation factors is conducted by a combined engineering team which includes various engineering disciplines. For example: 'if the same performance for the comparative system is required, the estimating rate will be 1.0; if the lower performance is required, the estimating rate will be the between 0.80 and 0.99; if the higher performance is required, the estimating rate will be the range of 1.01 and 1.20’. Table 6.4 describes the estimation factor description and the selected estimation range.

The evaluation is conducted as a combination of the MTBF (TF_n) of the comparative system and the weight factor (R_{ni}) of the evaluation factors as shown in Table 6.5. Equation 6.10 can be used for the confirmation of the reliability performance of the whole system.

Table 6.5 Reliability Performance Allocation Matrix

Comparative System		Reliability Performance Evaluation					
Subsystem	MTBF	System Complexity	System criticality	Operating Time	Operational Environment	Weight factor	Results
Sub 1	TF_1	R_{11}	R_{12}	R_{13}	R_{14}	$\prod_{i=1}^{4} R_{1i}$	$TF_1 \cdot \prod_{j}^{4} R_{1i}$
Sub 2	TF_2	R_{21}	R_{22}	R_{23}	R_{24}	$\prod_{i=1}^{4} R_{2i}$	$TF_2 \cdot \prod_{j}^{4} R_{2i}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Sub n	TF_n	R_{n1}	R_{n2}	R_{n3}	R_{n4}	$\prod_{i=1}^{4} R_{ni}$	$TF_n \cdot \prod_{j}^{4} R_{ni}$

R_{ni}: The evaluation rate for the reliability performance of the n^{th} subsystem;

$\{0.8 \leq R_{ni} \leq 1.2\}$

TF_n: MTBF of the n^{th} subsystem of the comparative system.

The reliability performance of the system to design is evaluated by Equation 6.10 and it shall be also satisfied with the operational availability performance:

$$MTBF_S = \left[\frac{1}{\sum_{i=1}^{n}\left(\frac{1}{TF_i \cdot \prod_j^4 R_{ij}}\right)}\right] \tag{6.10}$$

Where,

$MTBF_S$ = the MTBF of the system.

6.3.3.2 Maintainability Performance Allocation

A maintainability performance allocation method using the engineering judgement of the system engineering team for the comparative system selected is also presented in this section. Table 6.6 describes the evaluation factors and maintainability range of the subsystems. The maintainability evaluation of the subsystems includes three factors as the qualitative design characteristics that affect the repair and replacement time, such as accessibility, modularity and standardisation, but the factor can be added, depending on the complexity, criticality and possibly the maintenance time. The estimating range is also ± 20% for upgrade and downgrade as shown in Table 6.6. The estimation method is the same using the reliability matrix estimation (BS EN 50126-3, 2006; Eo et al., 2010).

Table 6.6 Maintainability Performance Allocation Factors

Evaluation Factor	Evaluation Methods	Evaluation Rating
Accessibility	The way that makes easier maintenance	0.8 – 1.2
Modularity	The way that divides maintenance action into primary and secondary maintenance level	0.8 - 1.2
Standardisation	The way that a part or component can be interchangeable with others	0.8 – 1.2

Table 6.6 describes the estimation factors and the quantitative evaluation rating and Table 6.7 describes the maintainability estimation matrix. The evaluation is conducted by the combination of the weight factors for the subsystem to allocate and the MTTR performance of the comparative subsystems.

Table 6.7 Maintainability Performance Allocation Matrix

Comparative System Performance		Maintainability Evaluation				
Subsystem	MTTR	testability	accessibility	standardisation	Weight factor	Results
Sub 1	TR_1	M_{11}	M_{12}	M_{13}	$\prod_{i=1}^{3} \mathrm{M}_{1i}$	$TR_1 \cdot \prod_{i}^{3} M_{1i}$
Sub 2	TR_2	M_{21}	M_{22}	M_{23}	$\prod_{i=1}^{3} \mathrm{M}_{2i}$	$TR_2 \cdot \prod_{i}^{3} M_{2i}$
…	…	…	…	…	…	…
Sub n	TR_n	M_{n1}	M_{n2}	M_{n3}	$\prod_{i=1}^{3} \mathrm{M}_{ni}$	$TR_i \cdot \prod_{i}^{3} M_{ni}$

M_{ni}: The evaluation rate for the maintainability factor of the *n*th subsystem;

$\{0.8 \leq M_{ni} \leq 1.2\}$

TR_n: MTTR of the *n*th subsystem of comparative system.

The maintainability of the whole system shall be confirmed by Equation 6.11: The $\mathrm{MTTR_S}$ should satisfy the maintainability and availability performance requirements:

$$MTTR_S = \frac{\sum_{i=1}^{n}\left(\frac{1}{TF_i \cdot \prod_j^4 R_{ij}} \cdot \frac{1}{TR_i \cdot \prod_j^3 M_{ij}}\right)}{\sum_{i=1}^{n}\left(\frac{1}{TF_i \cdot \prod_j^4 R_{ij}}\right)} \qquad (6.11)$$

Where,

$MTTR_\mathrm{S}$ = MTTR of the entire system to design.

6.3.4 Design RAMS Performance Definition Phase

This phase is a process that defines the RAMS performance design and acceptance criteria of the physical design architecture (components) comprising the system to design. It is started with identifying the design solution alternatives and developing the models and/or prototypes coherent to the alternatives of the design solutions. The models and prototypes are tested, analysed, fixed and retested repeatedly until the achievement of RAMS requirements and the test results are evaluated to verify the achievement of the RAMS acceptance performance criteria as shown in Figure 6.5. Therefore, RAMS design verification is an important activity in this process phase. The RAMS design verification is conducted to: (1) predict the RAMS performance for warranty costs and products, (2) compare the performances of functionally similar systems and (3) verify the compliance with specified RAMS requirements. The RAMS design verification is implemented by the growth assessment and demonstration of reliability performance as shown in Figure 6.9 (BS IEC 61124, 2006).

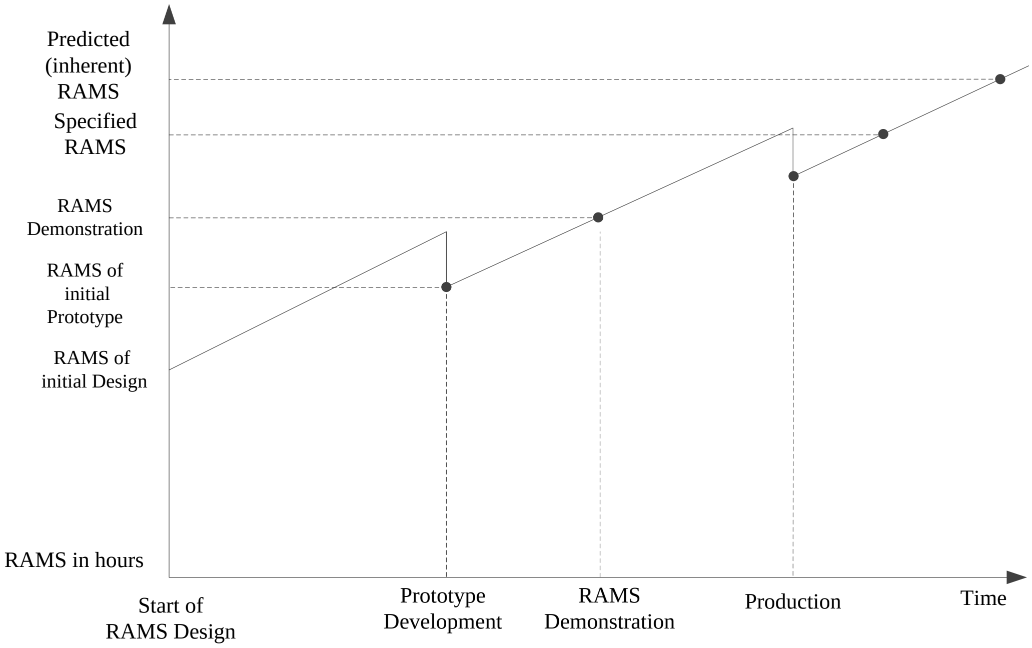


Figure 6.9 RAMS Growth Assessment and Verification Procedure

6.3.4.1 Reliability Performance Growth Assessment

Reliability growth assessment (RGA) is applied for the improvement of reliability performance through the systematic and permanent removal of the failure mechanism. The RGA aims to assess reliability performance over total time through design changes of the system. The RGA is accomplished through implementation of the test-analysis-fix-test cycle for system prototypes or modelling. It is intended for the improvement of reliability performance over test time to eliminate or minimise the deficiencies of the system design. The reliability growth is determined by the accumulated failure frequency over test time through design changes. The Duane model uses a deterministic approach to assess the reliability growth such that the system MTBF versus operating time represents an approximate straight line if applied on log-log paper. It is useful to plan the point of the reliability verification (Rooney et al., 2001; Ebeling, 2010; MIL-HDBK-189C, 2011).

As long as reliability improvement is implemented continuously, the Duane model can be mathematically expressed by Equation 6.12:

$$MTBF = \frac{T}{n(T)}$$

$$= kT^{\alpha} \tag{6.12}$$

Where,

T = the total system test time;

$n(T)$ = the accumulated failures for T;

k = the cumulative MTBF at T=1, and;

α = the typical growth rate.

Take the logarithms in Equation 6.12 to form the straight line as shown in Equation 6.13:

$$ln(MTBF) = ln\, k + \alpha lnT \tag{6.13}$$

When MTBF is plotted against ‘T’ on log/log paper, the points will form a straight line having a slope α. The angle of the slope ‘α’ means the growing degree of the reliability performance.

6.3.4.2 Reliability Performance Demonstration

There are many demonstration methods for reliability assessment of system design, but the truncated sequential test evaluation (TSTE) can generally be applied for the system design verification at the system concept design phase. The TSTE is a reliability demonstration technique that has been used to identify the achievement of reliability requirements, the reliability prediction for the design results and the provision of reliability acceptance criteria. The TSTE uses a designed evaluation graph to assess the achievement of reliability requirements as shown in Figure 6.10. Therefore, the design of the evaluation graph is very important to determine the reliability acceptance criteria. Thus, this section presents the method to design an evaluation graph as shown in Figure 6.10.

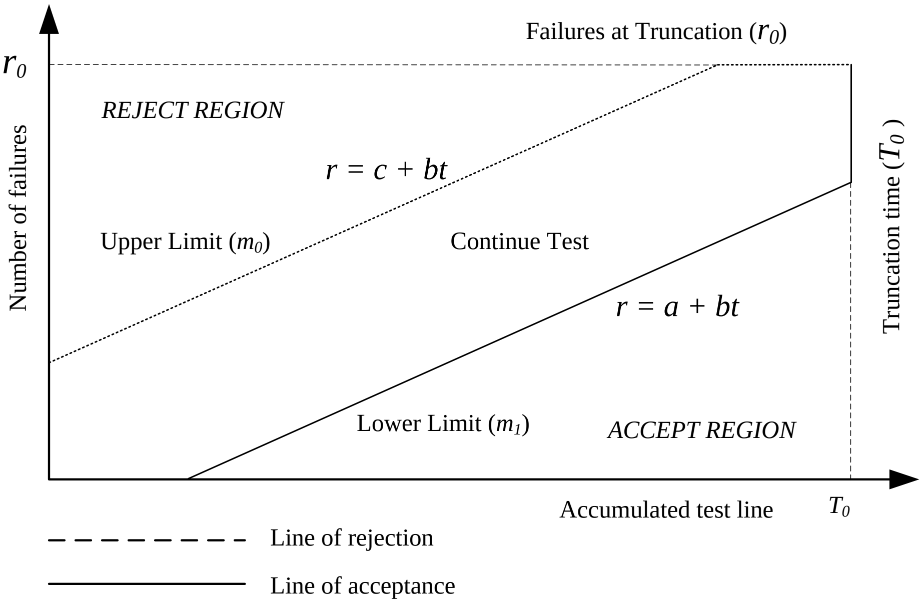


Figure 6.10 Truncated Sequential Test Evaluation Graph

The TSTE is based on the Poisson and Exponential distribution (Ebeling, 2010). “If the failure distribution of a system is Poisson distribution, the failure rate will be constant, and the failure frequency is independent of those of any other interval.” that is, during the test interval (*t*), the failure frequency (*r*) to occur will be observed continuously. Accordingly, “the probability, *P*(*r*), that the failure frequency (*r*) to occur will be observed over a test interval (t)” can be expressed as Equation 6.14 (BS EN 61124, 2006; MIL-HDBK-388B, 1984; David et al., 1952):

$$P(r) = \left(\frac{t}{m}\right)^r \left(\frac{e^{-t/m}}{r!}\right) \qquad (6.14)$$

If the unknown *MTBF*[23] (*m*) is equal to the lower limit *MTBF* (m_1), Equation 6.14 can be represented as Equation 6.15 to get the probability ($P_1(r)$):

$$P_1(r) = \left(\frac{t}{m_1}\right)^r \frac{exp(-t/m_1)}{r!} \qquad (6.15)$$

If the “*MTBF* (*m*)*”* is equal to the upper limit $MTBF(m_0)$, Equation 6.14 can be replaced by Equation 6.16 to get the probability ($P_0(r)$):

$$P_0(r) = \left(\frac{t}{m_0}\right)^r \frac{exp(-t/m_0)}{r!} \qquad (6.16)$$

The probability ratio ($P_r(r)$) between the two probabilities ($P_0(r)$ and $P_1(r)$) of Equations 6.15 and 6.16 is expressed by Equation 6.17 as follow:

$$P_r(r) = \frac{P_1(r)}{P_0(r)} \qquad (6.17)$$

If Equations 6.15 and 6.16 are applied to Equation 6.17, the result becomes Equation 6.18:

[23] MTBF which will be evaluated by the test

$$P_r(r) = \frac{P_1(r)}{P_0(r)} = \left(\frac{m_0}{m_1}\right)^r \cdot exp\left[-\left(\frac{1}{m_1} - \frac{1}{m_0}\right) \cdot t\right] \tag{6.18}$$

To continue the truncated sequential test, Equation 6.18 should be between the two constant values, A and B, as shown below:

$$B \leq P_r(r) \leq A \tag{6.19}$$

During this test, the probability ratio ($P_r(r)$) is evaluated and continuously compared to the two constant predetermined values, A and B. It should be satisfied according to the following decision rules:

- If $P_r(r) \leq B$, accept and stop testing;
- If $P_r(r) \geq A$, reject and stop testing, and;
- If $B < P_r(r) < A$, continue testing.

The constant values, A and B, of Equation 6.19 can be obtained by the risk of producer and customer and discrimination ratio as shown in Equations 6.20 and 6.21:

$$A = \frac{(1-\beta)}{\alpha} \cdot \frac{(D+1)}{2 \cdot D} \tag{6.20}$$

$$B = \frac{\beta}{(1-\alpha)} \tag{6.21}$$

Where:

α = Producer’s risk;

β = Customer’s risk, and;

D = Discrimination ratio.

In Equation 6.20, the equation, $[(D+1)/(2 \cdot D)]$ is a correction factor to better fulfil the nominal risks. The discrimination ratio (D) can be found by Equation 6.22 (BS EN 61124, 2006):

$$D = \frac{m_0}{m_1} = \frac{\lambda_1}{\lambda_0} \tag{6.22}$$

By the result of Equation 6.22, Equation 6.18 can be expressed as Equation 6.23:

$$P_r(r) = \frac{P_1(r)}{P_0(r)} = D^r \cdot exp\left[-\left(\frac{1}{m_1} - \frac{1}{m_0}\right) \cdot t\right] \tag{6.23}$$

Again, Equation 6.19 is applied to Equation 6.23 to get the constant A and B as shown below:

$$B \ < D^r \cdot exp\left[-\left(\frac{1}{m_1} - \frac{1}{m_0}\right) \cdot t\right] < A \tag{6.24}$$

Equation 6.24 can take 'natural logarithms' as Equation 6.25 to produce a straight line and facilitate the evaluation of the test results:

$$ln(B) < r \cdot ln(D) - \left(\frac{1}{m_1} - \frac{1}{m_0}\right) t < \ln(A) \tag{6.25}$$

If Equation 6.25 is divided by "*ln* (D) - $\left(\frac{1}{m_1} - \frac{1}{m_0}\right) \cdot t$", the result becomes Equation 6.26 as shown below:

$$\frac{ln(B)}{ln(D)} + \frac{\left(\frac{1}{m_1} - \frac{1}{m_0}\right)}{ln(D)} \cdot t < r < \frac{ln(A)}{ln(D)} + \frac{\left(\frac{1}{m_1} - \frac{1}{m_0}\right)}{ln(D)} \cdot t \tag{6.26}$$

Equation 6.26 can be simply replaced by Equation 6.27 as follows:

$$a + bt < r < c + bt \tag{6.27}$$

Where,

"$a + bt$" expresses the accept line of Figure 6.10 and;

"$c + bt$" expresses the reject line of Figure 6.10.

The constants: a, b and c in Equation 6.27 are expressed as shown below:

$$a = \frac{ln(B)}{ln(D)} \tag{6.28}$$

$$c = \frac{ln(A)}{ln(D)} \tag{6.29}$$

$$b = \frac{\left(\frac{1}{m_1} - \frac{1}{m_0}\right)}{ln(D)} = \frac{D - 1}{m_0 \cdot ln(D)} \tag{6.30}$$

The appropriate value of failure frequency (r) should be the smallest integer that can be used. Therefore, Equation 6.31 can be represented as follows:

$$\frac{x^2_{(1-\alpha);2r_0}}{x^2_{\beta;2r_0}} \geq \frac{m_1}{m_0} = \frac{1}{D} \tag{6.31}$$

Where $x^2_{(1-\alpha);2r_0}$ and $x^2_{\beta;2r_0}$ are chi-square variables with a $2r$[24] degree of freedom; these two values are identified by the $(1 - \alpha)$ and β probabilities of the chi-square tables, until the ratio of the variables is equal to or greater than "$1/D$". After this point is identified, the degrees of freedom are set as equal to $2r$. The value of r is rounded to the next highest integer. This value is r_0[25]. From this value, the truncation time (T_0) is calculated as Equation 6.32 (MIL-HDBK-388B, 1984):

[24] r: observed number of failures during the test

[25] r_0: truncated test failure number for sequential tests

$$T_0 = \frac{m_0 x^2_{(1-\alpha);2r_0}}{2} \tag{6.32}$$

The minimum test time ($T_{a.min}$) for acceptance without a test failure is:

$$T_{a.min} = -\frac{a}{b} \tag{6.33}$$

<u>An Example for Truncated Test Plan:</u>

The following gives an example to implement a truncated sequential test plan that assesses the reliability performance acceptance of the system design. The given data in the example is producer's risk (α), customer's risk (β), lower limit (m_1) and upper limit (m_0) as below:

$$\alpha = 0.10 \tag{6.34}$$

$$\beta = 0.10 \tag{6.35}$$

$$m_1 = 100\ hours \tag{6.36}$$

$$m_0 = 200\ hours \tag{6.37}$$

For the above given data, the values for designing a test evaluation graph: i.e., the discrimination ratio, accept-reject criteria, truncation points, and the scope and ordinate intercepts of the test plan can be determined:

The solution derived is given below:

$$D = \frac{m_0}{m_1} = \frac{200}{100} = 2 \tag{6.38}$$

$$A = \frac{(d+1)(1-\beta)}{2ad} = \frac{(2+1)(1-0.10)}{2(2)(0.10)} = 6.75 \tag{6.39}$$

$$B = \frac{\beta}{(1-\alpha)} = \frac{0.10}{(1-0.10)} = 0.111 \qquad (6.40)$$

$$\frac{x^2_{(1-\alpha);2r}}{x^2_{\beta;2r}} = \frac{x^2_{0.9;2r}}{x^2_{0.1;2r}} \geq \frac{m_1}{m_0} = \frac{1}{2} \qquad (6.41)$$

Equation 6.41 can find at 29 degrees of freedom at the chi-square table. Therefore, Equation 6.41 can be represented as Equation 6.42:

$$\frac{x^2_{0.9;2r}}{x^2_{0.1;2r}} = \frac{19.763}{39.087} = 0.506 \qquad (6.42)$$

Therefore:

$2r = 29$

$r = 14.5$

$r_0 = 15$ failures

In addition, the total truncated test time is as shown below:

$$T_0 = \frac{m_0 x^2_{(1-\alpha):2r}}{2}$$

$$= \frac{200(20.6)}{2}$$

$$= 2{,}060\ hours \qquad (6.43)$$

By the above results, the test can be predicted that the failure frequency does not excess 15 failures and the test time does not last longer than 2060 hours.

To determine the slope and ordinate intercepts of the two parallel straight lines:

$$a = \frac{lnB}{ln(\frac{m_0}{m_1})} = \frac{ln\,0.111}{ln2} = \frac{-2.108}{0.693} = -3.17 \qquad (6.44)$$

$$b = \frac{(\frac{1}{m_1} - \frac{1}{m_0})}{ln(\frac{m_0}{m_1})} = \frac{(0.01 - 0.005)}{ln2} = 0.00721 \tag{6.45}$$

$$c = \frac{lnA}{ln(\frac{m_0}{m_1})} = \frac{ln\,6.75}{ln2} = \frac{1.910}{0.693} = 2.75 \tag{6.46}$$

Therefore, the following evaluation graph is obtained for TSTE:

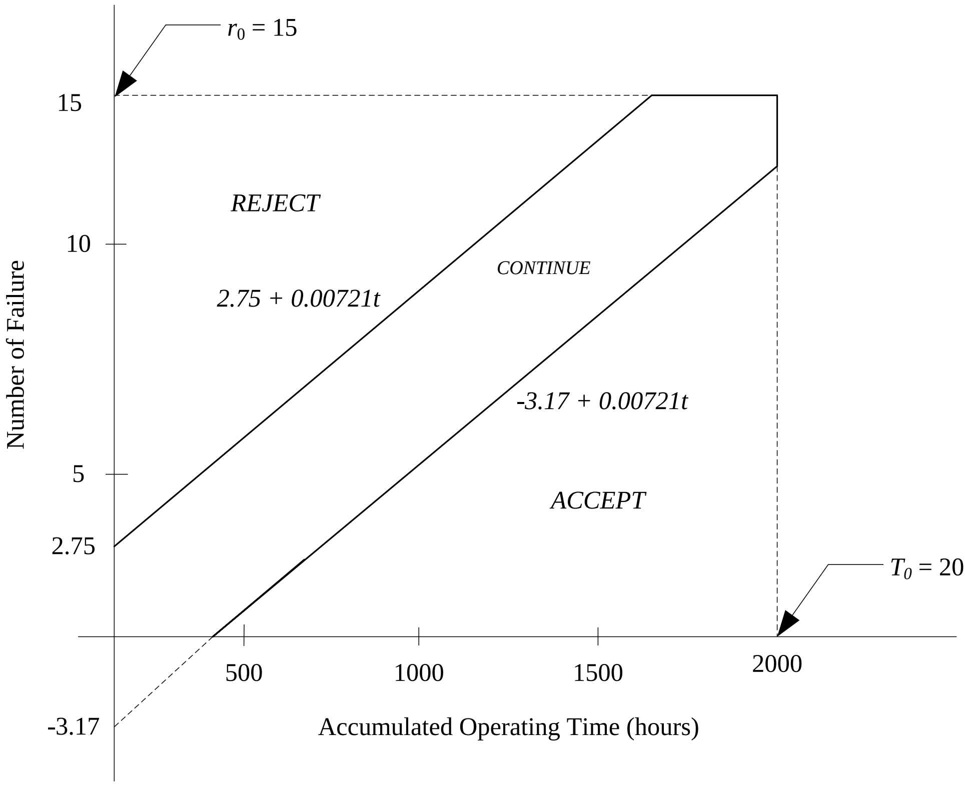


Figure 6.11 Planed Truncated Sequential Test Evaluation Graph

6.4 Summary

This chapter has presented the method that develops railway RAMS performance specification appropriate to RAMS requirements and operational applications to provide RAMS design solutions and their acceptance performance criteria for the implementation of the systems design efforts and/or contract. It has also discussed a RAMS performance specification process to ensure the high feasibility of railway RAMS design solutions in the system operation and maintenance phase.

This chapter firstly presented a framework that specifies RAMS requirements and operational contexts. The framework provided five specification factors: (1) the establishment of railway service objectives, (2) the definition of the railway RAMS concept, (3) the establishment of RAMS performance specification principle, (4) the selection of RAMS measures and (5) the development of the RAMS performance specification process. These are essential factors for the development of the RAMS performance specification.

This chapter secondly provided a process model that specifies the RAMS requirements and operational applications. The process consisted of an input and three process phases based on the systems engineering process. The operational definition phase provided the detailed process activities and techniques as a basis for the overall specification process. However, each process phase has specific process activities. Thus, this chapter focused on the specific process activities and techniques such as operational behaviour assessment, RAMS allocation, RAMS performance verification etc.

In conclusion, RAMS performance specification is an essential RAMS management effort to be conducted at the system concept design phase in order to facilitate the system design efforts and ensure the feasibility of the system design in the operational phase. Accordingly, the proposed framework and process will effectively support the development of railway RAMS performance specification.

Chapter 7

CASE STUDY

7.1 Introduction

Case study is a practical research method to find the effective solutions of the research issues derived from the research subjects. The case study can also expand the range of knowledge, experience and know-how related to the research, and the results achieved from the case study can improve or update the results that have already been acquired. Therefore, this chapter provides a case study for the application of the risk assessment to rail vehicle pneumatic braking unit (RAPBU). It aims to demonstrate the application of the proposed FMEA-FTA based risk assessment method and to investigate the reliability performance, the failure events, and their failure causes related to RAPBU.

The braking equipment takes the roles of stopping the rail vehicle at the station to provide the rail traffic service, reducing the running speed of the rail vehicle whenever required by the signalling or driver's master controller; and keeping the rail vehicle at a specific place for maintenance or parking. There are different kinds of rail vehicle brakes, for example, mechanical, thermal, pneumatic, electrical brake etc., depending on the type of the rail vehicle. The pneumatic brake has a basic and back up function for the other braking and it also has an braking function for response to the emergency situations. Therefore, RAPBU is one of the safety critical equipment of a rail vehicle system and its risk level is a key decision making factor for RAMS management in the system design and development phase (Ting et al., 2011).

This chapter consists of five sections to provide a case study for risk assessment of RAPBU. Section 7.2 describes the system structure and function of the RAPBU. The risk assessment based on FMEA and FTA techniques is performed in Section 7.3 and the results of the risk assessment are discussed in Section 7.4. This chapter finally provides a brief summary in Section 7.5.

7.2 Rail Vehicle Pneumatic Braking

7.2.1 Pneumatic Braking Description

The brake operation of rail vehicle is a very complex process specific to rail vehicles; it is a important safety function which takes charge of controlling the operating speed of a rail vehicle and stopping it at the fixed position of a station for passenger or freight service. During the brake operation of the braking equipment, the different kinds of braking functions, such as mechanical, thermal, pneumatic, electrical etc., can take place together. The pneumatic braking always takes place at various points as a basic, back up or emergency function whenever required from signalling or driver (Zang et al., 2010; Cha, 2010).

The major objectives of the pneumatic braking function are to perform the followings:

- Perform the controlled reduction in speed of the rail vehicle;
- Reach a certain lower operating speed as soon as possible;
- Stop at a fixed point, or;
- Suddenly stop at any point in an emergency situation of the rail vehicle or the rail track.

7.2.2 Pneumatic Braking Structure

Figure 7.1 shows the simplified structure related to the rail vehicle pneumatic braking, which is located under the car body to control the braking air pressure of the braking cylinder. The pneumatic braking assembly consists of five components as shown in Figures 7.1 and 7.2: (1)

air filter (AF), (2) braking control unit (BCU) assembly, (3) oil separator (OS), (4) automatic drain valve (ADV) and (5) dump valve (DV).

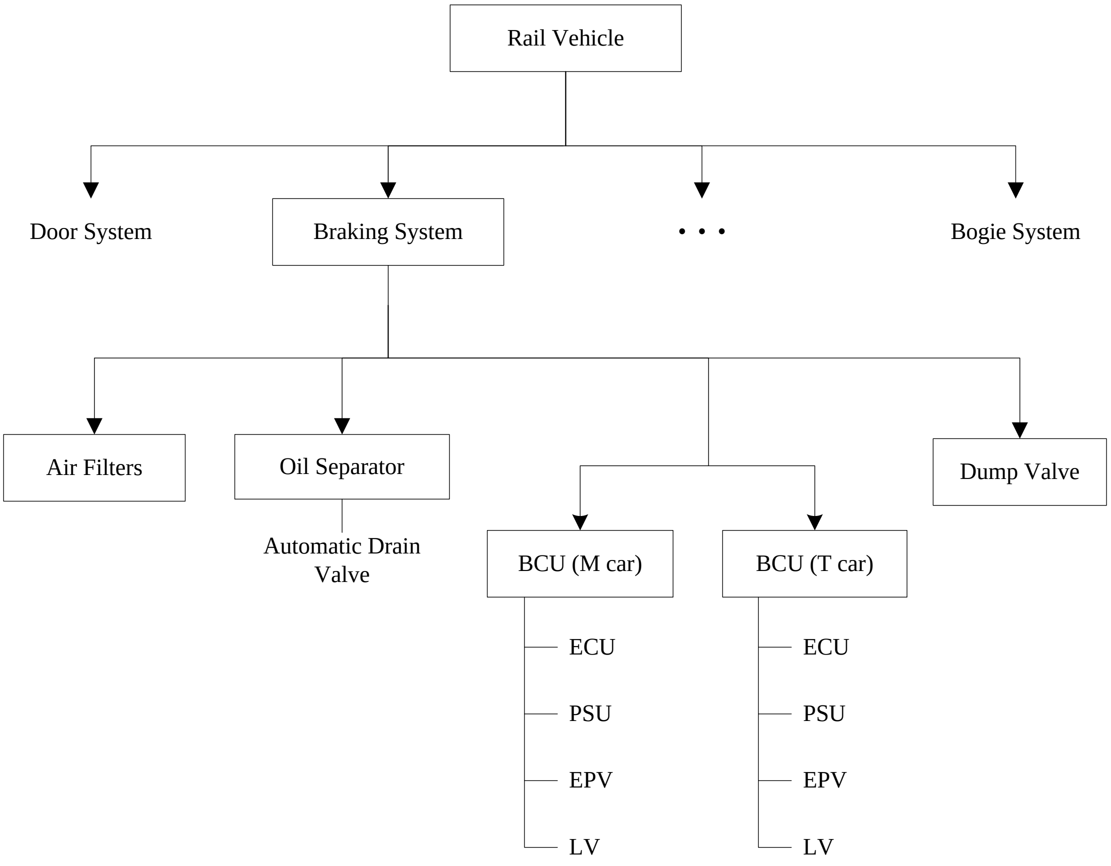


Figure 7.1 Pneumatic Braking Structures

The AF takes the role of filtering impurities included in the braking air provided from the main air reservoir. The BCU assembly has a function that controls the amount of braking air as a main assembly of the pneumatic braking unit. The ADV separates water or oil involved in the braking air and the DV instantaneously controls the air brake force to prevent the train wheels skidding and flatted wheels, to always keep the same braking distance and to maintain the passenger safety. The information below briefly gives the overall functions of the pneumatic braking unit. Figure 7.1 briefly describes the train brake structure related to the PBU and Table 7.1 provides a functional description of the PBU.

Table 7.1 Function Description of Pneumatic Braking Unit

No	Subsystem	Function description
01	Air filter (AF)	To filter impurities, such as dust, from the main air reservoir
02	Electrical Control Unit (ECU)	To control the braking force of a rail vehicle which is commanded by the operator or ATC computer, including the passenger load and braking pattern. It aims to keep a constant braking distance, irrespective of the rail vehicle's operating speed.
03	Electric - Pneumatic Change Relay Valve (EPV)	To control the air pressure of the braking cylinder. It is controlled by two magnet control flow valves. The EPV controls service braking and emergency braking.
04	Load Valve (LV)	To sense the passenger load weight of the rail vehicle needed to control the braking force of the rail vehicle.
05	Pressure Sensing Unit (PSU)	To calculate the passenger load of the rail vehicle, and senses the air pressure of the braking cylinder.
06	Oil Separator (OS)	The OS takes the role of separating water and oil from the air used in braking.
07	Automatic Drain Valve (ADV)	To separate water and oil from the main air reservoir when the air compressor is stopped
08	Dump Valve (DV)	To prevent a flat wear of the rail vehicle's steel wheel and the increase of the braking distance due to the wheel skid of the rail vehicle

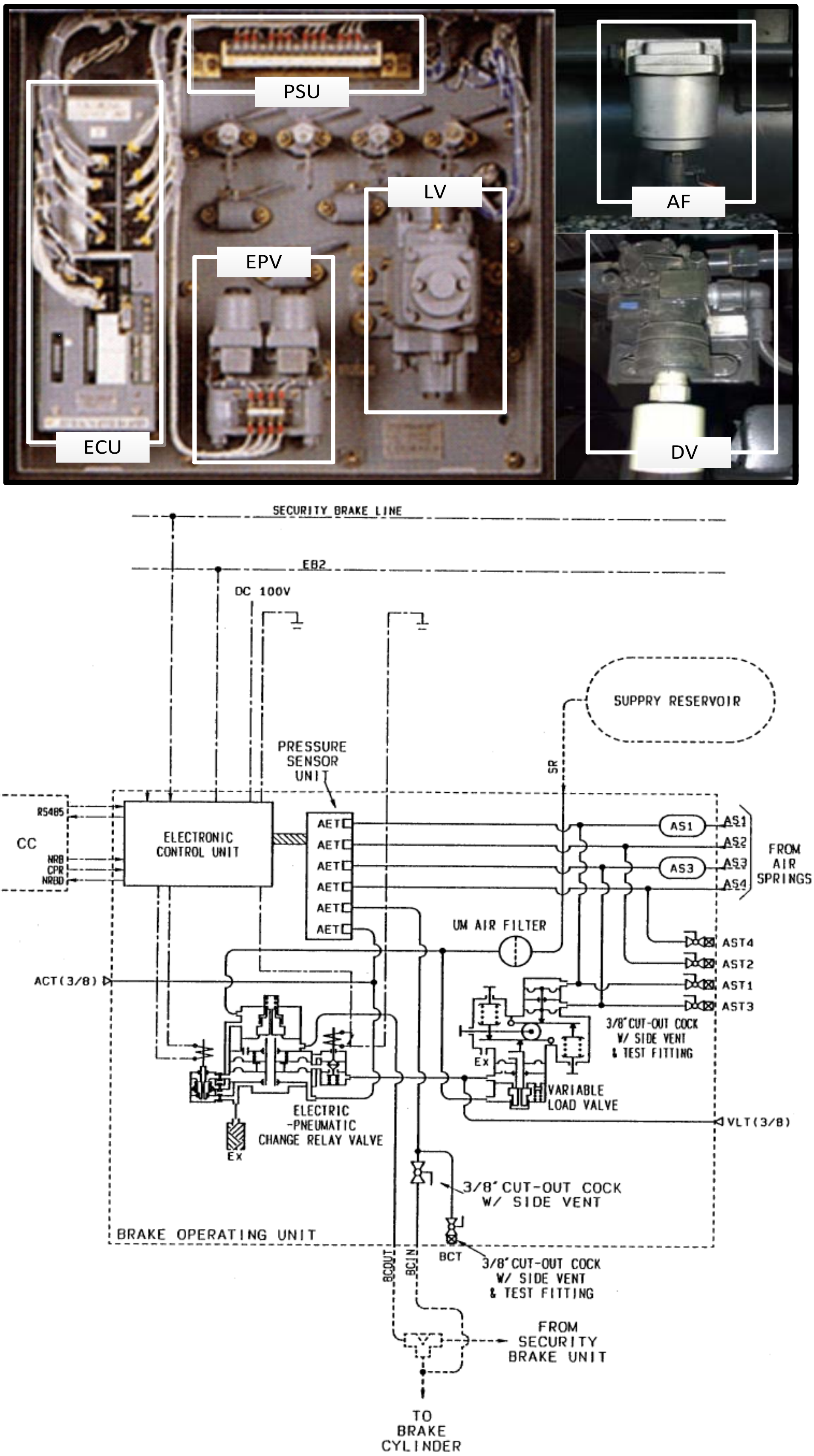


Figure 7.2 Pneumatic Braking Pictures and Drawing

7.2.3 Pneumatic Braking Function

Figure 7.3 shows the functional block diagram (FBD) that describes the overall pneumatic braking function associated with the PBU, which is comprised of three parts: (1) Central Braking Control (CBC), (2) Pneumatic Braking Control (PBC) and (3) Pneumatic Braking Operation (PBO). The CBC plays the role of the central braking force control of the entire train system and it consists of four control units: Master Controller (MC), Automation Train Control (ATC), Train Computer (TC) and Car Computer (CC), as shown in Figure 7.3.

The ATC implements the automatic braking/releasing command, depending on the allowed speed signalling detected from the rail track signal system. The TC calculates the brake force pressure needed for the brake operation of the whole train and it also controls the brake force pressure for each train car. The CC is the central braking control unit of a train car and it calculates the air brake force pressure that controls the pneumatic braking unit.

The PBC is the central braking control unit as the PBU of a train car; it is equipped in every train car to control the braking air pressure according to the braking or releasing command of the car computer. As seen in Figure 7.3, PBC also controls the amount of brake air of the brake cylinder for the generation of the air brake force pressure, which is balanced through checking of the air brake force pressure, the passenger load, the cross blending and the jerk control for passenger safety. The dump valve helps the safe braking function of the PBC through controlling the working time of the air brake force pressure to keep the same braking distance. The air spring signalling, which indicates the number of passengers (total passenger weight) boarded in the rail vehicle, is an important force in determining the air brake force pressure.

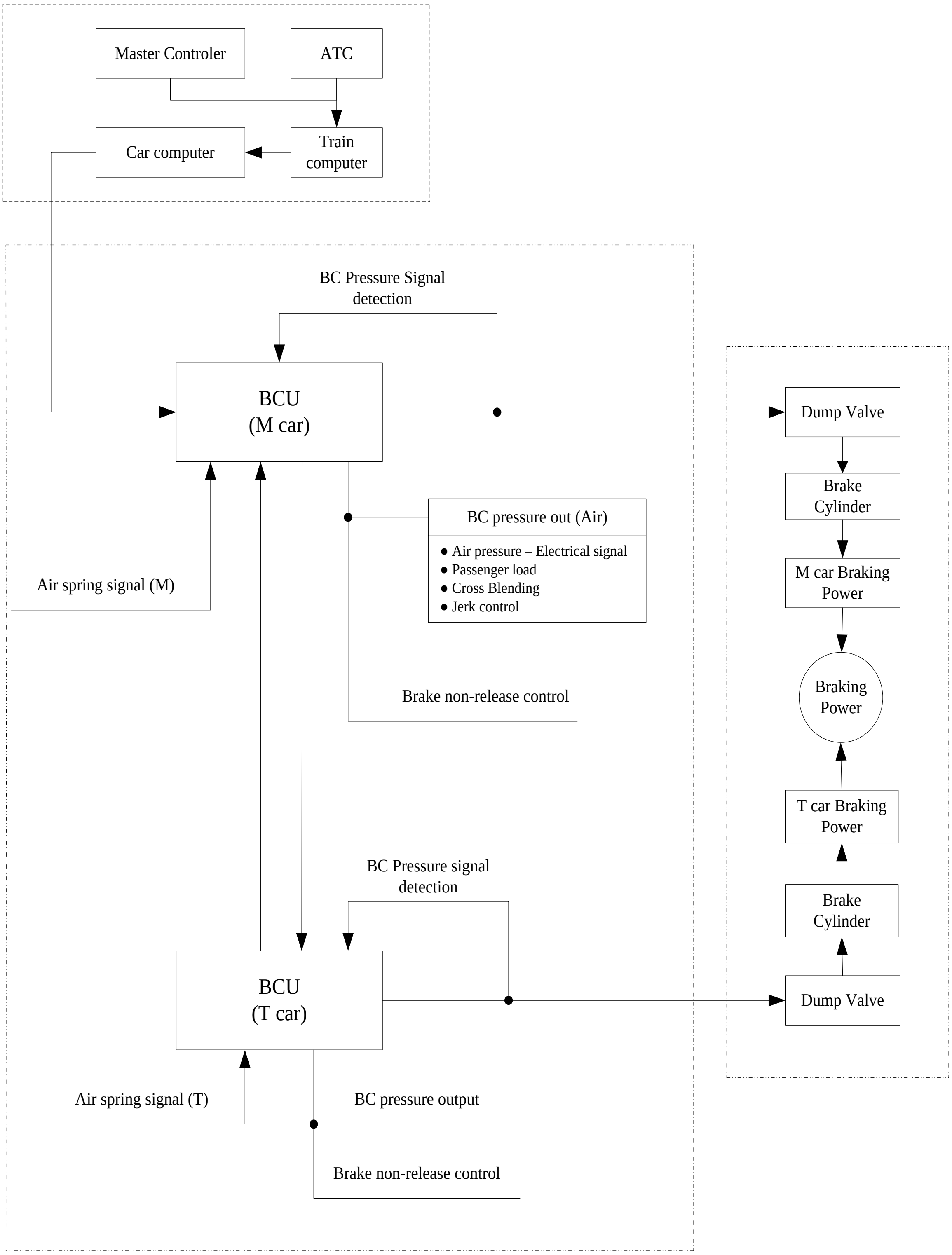


Figure 7.3 Pneumatic Braking Functional Block Diagram

7.3 Risk Assessment of Pneumatic Braking Unit

7.3.1 Data Collection and Data Analysis

The failure data stored in the failure collection system over a specific period are assembled to determine the necessary inputs which carry out the RAMS risk assessment of the pneumatic braking unit. This failure data has been reviewed from the system descriptions of rail vehicle as presented by Kim (2008). The failure causes were further examined to identify the minimal cut sets and the risk level. Table 7.2 describes the failure/operation data collected from railway field.

Table 7.2 Collected PBU Failure/Operation Data

<table>
<tr><th>Failure Code</th><th>Subsystem</th><th colspan="2">Component Failure Mode</th><th>Failure Frequency</th><th>Operation Distance (<i>km</i>)</th></tr>
<tr><td>P-1</td><td rowspan="2">AF</td><td colspan="2">Air filter leakage</td><td>10</td><td>4,546,307.4</td></tr>
<tr><td>P-2</td><td colspan="2">Automatic drain valve failed</td><td>16</td><td>8,957,986</td></tr>
<tr><td>P-3</td><td rowspan="2">LV</td><td colspan="2">LV pressure change</td><td>16</td><td>8,178,184.8</td></tr>
<tr><td>P-4</td><td colspan="2">LV short</td><td>4</td><td>1,830,344.9</td></tr>
<tr><td>P-5</td><td rowspan="2">PSU</td><td colspan="2">PSU sensing error</td><td>67</td><td>22,451,193.9</td></tr>
<tr><td>P-6</td><td colspan="2">PSU short</td><td>22</td><td>7,875,822.1</td></tr>
<tr><td>P-7</td><td rowspan="3">ECU</td><td colspan="2">ECU in/output fail</td><td>1</td><td>438,907.9</td></tr>
<tr><td>P-8</td><td colspan="2">Communication error</td><td>197</td><td>43,126,168.4</td></tr>
<tr><td>P-9</td><td colspan="2">Power supply error</td><td>25</td><td>10,932,356.2</td></tr>
<tr><td>P-2</td><td rowspan="5">EPV</td><td colspan="2">Automatic drain valve failed</td><td>16</td><td>8,957,986</td></tr>
<tr><td>P-10</td><td colspan="2">Pressure sensing error</td><td>49</td><td>8,499,257.5</td></tr>
<tr><td>P-8</td><td colspan="2">Communication error</td><td>197</td><td>43,126,168.4</td></tr>
<tr><td>P-11</td><td rowspan="2">EPV function error</td><td>EPV leakage</td><td>5</td><td>1,237,982.5</td></tr>
<tr><td>P-12</td><td>Dreg in EPV</td><td>88</td><td>16,349,332.0</td></tr>
</table>

7.3.2 Definition of Risk Assessment Parameter and Evaluation Matrix

To assess the risk level of the PBU, three risk evaluation factors are defined: (1) the failure severity and the failure frequency parameters to evaluate the failure consequence; (2) risk level parameter to determine the risk control and (3) a risk evaluation matrix to determine the risk level. The descriptions of the risk evaluation factors to evaluate the railway vehicle risks are altered from Table 5.1 to 5.2 of Chapter 5, as described in Table 7.3, 7.4 and 7.5. Table 7.6 describes the risk evaluation matrix to determine the risk level of PBU.

Table 7.3 Failure Severity Parameters

Risk Category	Consequence to Service	Level
Catastrophic	Multiple vehicles delay for extended period due to the loss of many major systems.	4
Critical	Single vehicle delays for extended period. The vehicle was removed from service or sections of track missed/by passed due to the loss of a major system.	3
Marginal	Single or multi-vehicles delayed for short time period (possible catch up mode) due to severe system (s) damage.	2
Insignificant	System delays less than minutes due to minor system damage.	1

Table 7.4 Risk Level Parameters

Risk classification	Risk Level	Risk Reduction/Control
Intolerable	4	Risk shall be eliminated.
Undesirable	3	Risk shall only be accepted when risk reduction is impracticable and with agreement.
Tolerable	2	Risk is acceptable with adequate control and agreement.
Negligible	1	Acceptable without any agreement.

Table 7.5 Failure Frequency Parameters

Frequency Classification		Description	Frequency	Level
F1	Frequent	It is likely to occur frequently and will be continually experienced.	$\geq 10^{-3}$	6
F2	Probable	It will occur several times and can be expected to occur often.	$10^{-4} <$ to $\leq 10^{-3}$	5
F3	Occasional	It is likely to occur several times and can be expected to occur several times.	$10^{-6} <$ to $\leq 10^{-4}$	4
F4	Remote	It is likely to occur sometime in the system life cycle and can reasonably be expected to occur.	$10^{-8} <$ to $\leq 10^{-6}$	3
F5	Impossible	It is unlikely to occur but is possible and it can be assumed that it may exceptionally occur.	$10^{-9} <$ to $\leq 10^{-8}$	2
F6	Incredible	It extremely unlikely to occur and it can be assumed that it may not occur.	$\leq 10^{-9}$	1

Table 7.6 Risk Evaluation Matrix

Frequency Level		Risk Level			
Frequent	6	Undesirable	Intolerable	Intolerable	Intolerable
Probable	5	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	4	Tolerable	Undesirable	Undesirable	Intolerable
Remote	3	Negligible	Tolerable	Undesirable	Undesirable
Improbable	2	Negligible	Negligible	Tolerable	Tolerable
Incredible	1	Negligible	Negligible	Negligible	Negligible
		1	2	3	4
		Insignificant	Marginal	Critical	Catastrophic
		Severity Level of Failure Consequence			

7.3.3 Failure Consequence Analysis

Failure consequence analysis (FCA) is performed through analysing the failure modes of the PBU components and it determines the failure severity level of all possible failure consequences. Table 7.7 describes the failure consequence analysis to determine the failure severity level of the PBU.

Table 7.7 Failure Consequence Analysis of PBU

<table>
<tr><th rowspan="2">Failure Code</th><th rowspan="2">Sub-system</th><th rowspan="2" colspan="2">Component Failure mode</th><th colspan="3">Failure Consequence</th><th rowspan="2">Failure Severity</th></tr>
<tr><th>Component</th><th>Subsystem</th><th>System</th></tr>
<tr><td>P-1</td><td rowspan="2">AF</td><td colspan="2">Air filter leakage</td><td>function loss</td><td>function reduction</td><td>function reduction</td><td>2</td></tr>
<tr><td>P-2</td><td colspan="2">Automatic drain valve fail</td><td>function loss</td><td>function loss</td><td>function reduction</td><td>2</td></tr>
<tr><td>P-3</td><td rowspan="2">LV</td><td colspan="2">LV pressure change</td><td>function loss</td><td>function loss</td><td>function reduction</td><td>2</td></tr>
<tr><td>P-4</td><td colspan="2">LV short</td><td>function loss</td><td>function loss</td><td>function reduction</td><td>2</td></tr>
<tr><td>P-5</td><td rowspan="2">PSU</td><td colspan="2">PSU sensing error</td><td>function loss</td><td>function loss</td><td>function reduction</td><td>2</td></tr>
<tr><td>P-6</td><td colspan="2">PSU short</td><td>function loss</td><td>function loss</td><td>function reduction</td><td>2</td></tr>
<tr><td>P-7</td><td rowspan="3">ECU</td><td colspan="2">ECU in/output fail</td><td>function loss</td><td>function loss</td><td>function loss</td><td>3</td></tr>
<tr><td>P-8</td><td colspan="2">Communication error</td><td>function loss</td><td>function loss</td><td>function loss</td><td>3</td></tr>
<tr><td>P-9</td><td colspan="2">Power supply error</td><td>function loss</td><td>function loss</td><td>function loss</td><td>3</td></tr>
<tr><td>P-2</td><td rowspan="5">EPV</td><td colspan="2">Automatic drain valve failed</td><td>function loss</td><td>function reduced</td><td>function reduction</td><td>2</td></tr>
<tr><td>P-10</td><td colspan="2">Pressure sensing error</td><td>function loss</td><td>function reduced</td><td>function reduced</td><td>2</td></tr>
<tr><td>P-8</td><td colspan="2">Communication error</td><td>function loss</td><td>function loss</td><td>function loss</td><td>3</td></tr>
<tr><td>P-11</td><td rowspan="2">EPV function error</td><td>EPV leakage</td><td>function loss</td><td>function loss</td><td>function loss</td><td>3</td></tr>
<tr><td>P-12</td><td>Dreg in EPV</td><td>function loss</td><td>function loss</td><td>function loss</td><td>3</td></tr>
</table>

7.3.4 Failure Frequency Analysis

7.3.4.1 Fault Tree Construction

Fault tree is the most critical aspect in the failure frequency analysis and it is a prerequisite for the risk assessment. The fault tree is required for the quantitative and qualitative analysis of the failure frequency. Table 7.8 shows the relationship between the component failure modes and their basic events given from the failure analysis of the FMEA. The subsystem failure modes are the failure causes of a top event that causes "full service braking error of rail vehicle" and the component failure modes are the failure causes that lead to the subsystem failure. Figure 7.8 describes the failure cause scenario model for the component failure modes.

Table 7.8 Basic Event Definition for PBU Failure Modes

Subsystem Failure Mode	Component Failure Mode		Failure rate	Basic Event
AF function loss (A_1)	Air filter leakage		$F(X_1)$	X_1
	Automatic drain valve fail		$F(X_2)$	X_2
LV sensing error (A_2)	LV pressure change		$F(X_3)$	X_3
	LV short		$F(X_4)$	X_4
PSU sensing error (A_3)	PSU sensing error		$F(X_5)$	X_5
	PSU short		$F(X_6)$	X_6
ECU function error (A_4)	ECU in/output fail		$F(X_7)$	X_7
	Communication error		$F(X_8)$	X_8
	Power supply error		$F(X_9)$	X_9
EPV function error (A_5)	Automatic drain valve fail		$F(X_2)$	X_2
	Pressure sensing error		$F(X_{10})$	X_{10}
	Communication error		$F(X_8)$	X_8
	EPV function error (A_6)	Dregs in EPV	$F(X_{11})$	X_{11}
		EPV leakage	$F(X_{12})$	X_{12}

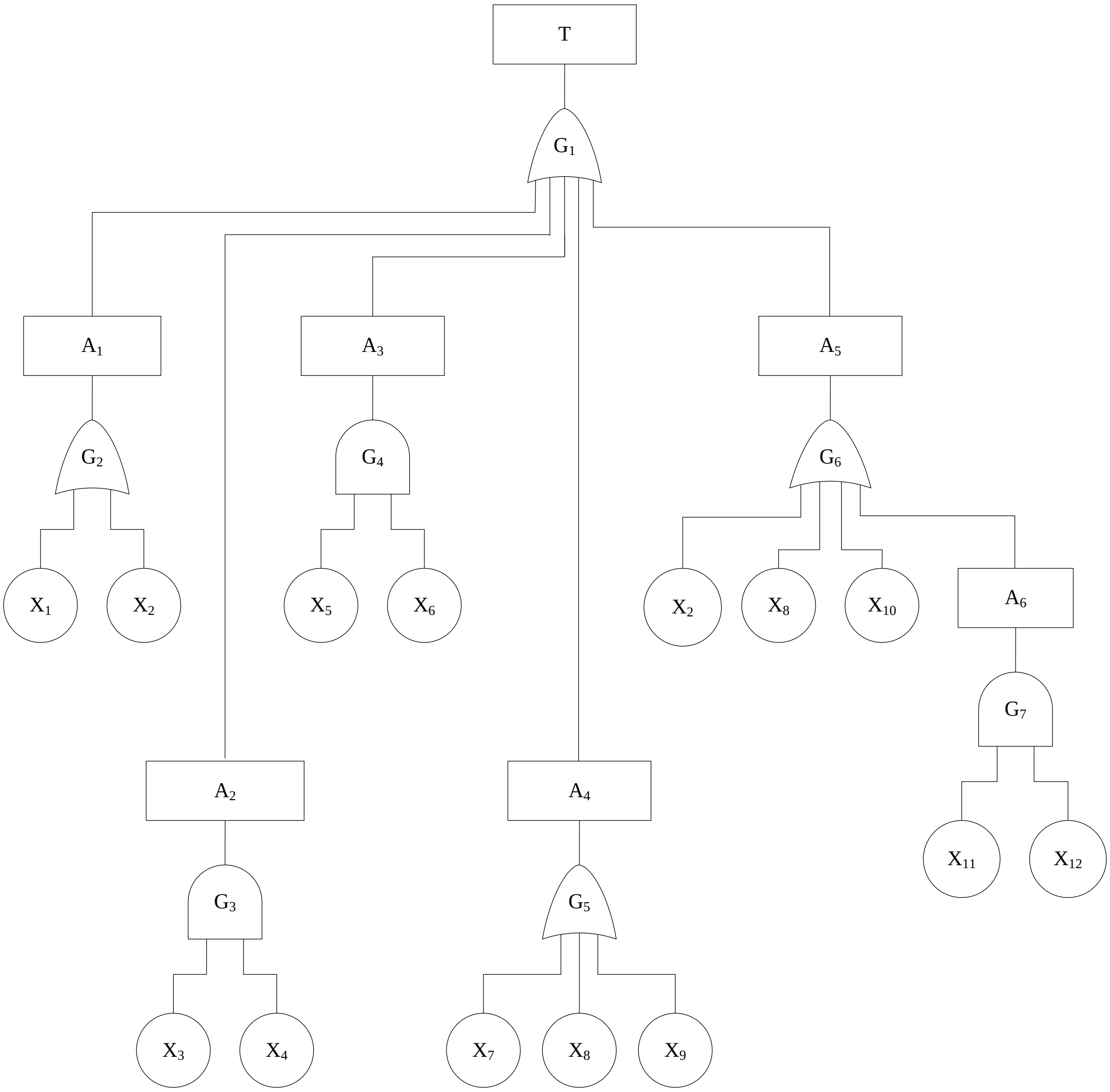


Figure 7.4 Fault Tree of Pneumatic Braking Unit

The top event “full - service braking operation error of rail vehicle” (T) can occur whenever any subsystem among five failure events (A_1, A_2, A_3, A_4, and A_5) is failed. Therefore, the top event (T) is connected by the ‘OR’ gate (G_1) from the lower failure events. The AF function error (A_1) has two failure causes (X_1, X_2) and it is not operated by only one failure cause (X_1 or X_2). So the A_1 is connected by the ‘OR’ gate (G_2) from the two failure causes (X_1, X_2). The LV sensing error (A_2) is brought about by the two failure causes (X_3, X_4) and it does not work when the two failure causes (X_3 and X_4) occur at the same time. Accordingly, the A_2 is connected by the 'AND' gate (G_3) as shown in Figure 7.4.

The PSU sensing error (A_3) has two failure causes (X_5, X_6) and it does not work when the two failures (X_5 and X_6) occur simultaneously. Thus, the A_3 has the 'AND' gate (G_4). The ECU function error failure event (A_4) occurs due to the three failure causes (X_7, $X_{8,}$ and X_9) and it does not function if any failure cause ($X_{7,}$ $X_{8,}$ or X_9) occurs. Therefore, the A_4 has the 'OR' gate (G_5) for the three failure causes.

The EPV function error (A_5) has three root failure causes (X_2, X_8 or $X_{10)}$ and an intermediate event (A_6). It does not work when four failures (X_2, $X_{8,}$ X_{10} or A_6) occur simultaneously. Accordingly, the A_5 has 'OR' gate (G_6). The intermediate event (A_6) of the EPV function error is brought about by two failure causes (X_{11} , X_{12}) and the failure event occurs through the two failure causes, so the A_6 is connected by 'AND' gate (G_7) as shown in Figure 7.4.

7.3.4.2 Qualitative Fault Tree Analysis

The qualitative fault tree analysis is an iterative procedure that determines the minimal cut sets (MCSs) using the Boolean algebra rules. The fault tree of Figure 7.4 can be represented by Equation 7.1 as blow:

$$T = A_1 + A_2 + A_3 + A_4 + A_5 \tag{7.1}$$

$$A_1 = X_1 + X_2 \tag{7.2}$$

$$A_2 = X_3 \cdot X_4 \tag{7.3}$$

$$A_3 = X_5 \cdot X_6 \tag{7.4}$$

$$A_4 = X_7 + X_8 + X_9 \tag{7.5}$$

$$A_5 = X_2 + X_8 + X_{10} + A_6 \tag{7.6}$$

$$A_6 = X_{11} \cdot X_{12} \tag{7.7}$$

Equation 7.1 can be replaced by Equations 7.2, 7.3, 7.4, 7.5, 7.6 and 7.7; as a result, the minimal cut sets of Figure 7.4 can be obtained by the Boolean algebra rules as Equation 7.8:

$$\begin{aligned} T &= (X_1 + X_2) + (X_3 \cdot X_4) + (X_5 \cdot X_6) + (X_7 + X_8 + X_9) + \{(X_2 + X_8 + X_{10}) + A_6\} \\ &= X_1 + X_2 + X_3 \cdot X_4 + X_5 \cdot X_6 + X_7 + X_8 + X_9 + X_2 + X_{10} + X_8 + X_{11} \cdot X_{12} \\ &= X_1 + (X_2 + X_2) + X_3 \cdot X_4 + X_5 \cdot X_6 + X_7 + (X_8 + X_8) + X_9 + X_{10} + X_{11} \cdot X_{12} \\ &= (X_1 + X_2) + (X_3 \cdot X_4) + (X_5 \cdot X_6) + (X_7 + X_8 + X_9) + \{X_{10} + (X_{11} \cdot X_{12})\} \quad (7.8) \end{aligned}$$

The minimal cut sets for the fault tree of Figure 7.4 can be simply expressed as described in Figure 7.5. As seen in Figure 7.5 and Equation 7.8, the top event “full - service braking operation error of rail vehicle” can be represented by nine minimal cut sets. The top event has six single point failures and three double point failures. The six single failures directly affect the top event. Table 7.9 shows the minimal cut sets of the pneumatic braking unit.

Table 7.9 Minimal Cut Sets of PBU

Category	Minimal Cut Sets	Set
1 MCS for basic event	(X_1), (X_2), (X_7), (X_8), (X_9), (X_{10})	6
2 MCS for basic event	(X_3, X_4), (X_5, X_6), (X_{11}, X_{12})	3
Total MCS		9

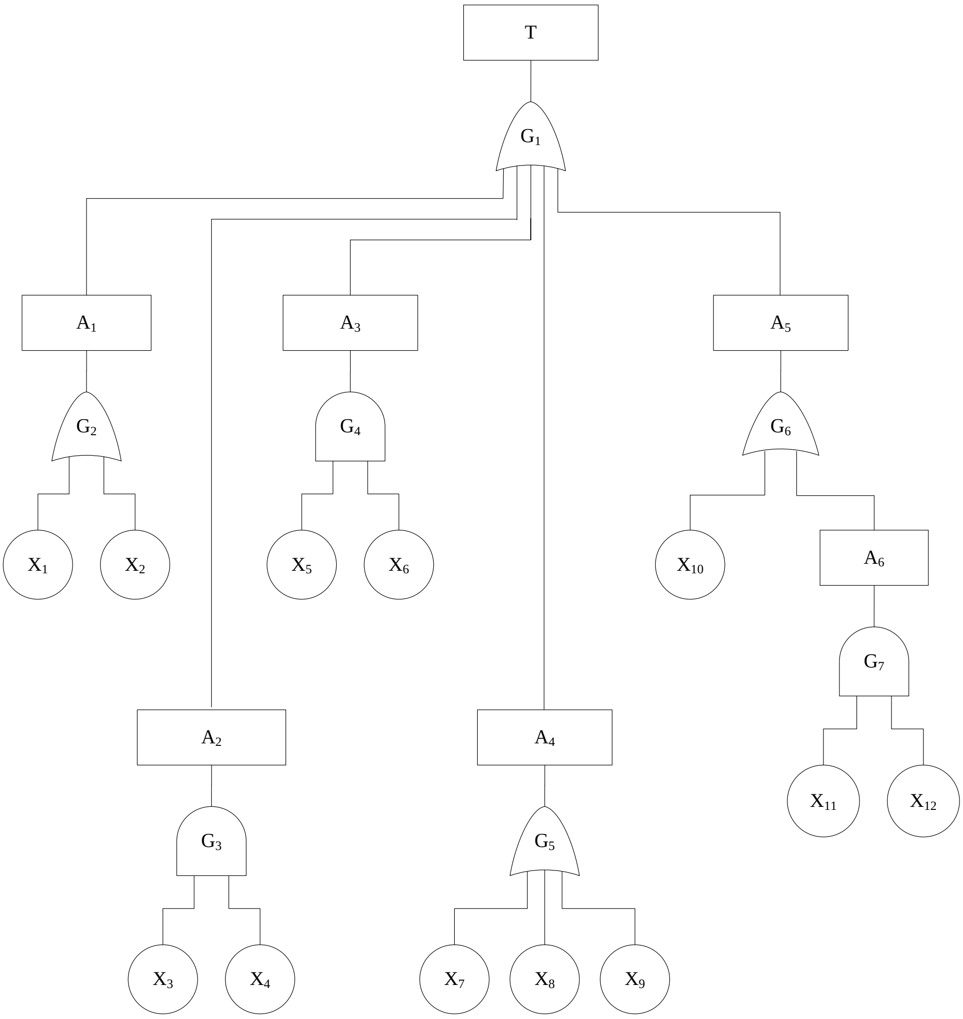


Figure 7.5 Fault Tree Simplified from Figure 7.4

7.3.4.3 Quantitative Fault Tree Analysis

Equation 7.8 simplified by the Boolean algebra rules can be quantified by the probability law or failure rate. Table 7.10 shows the failure data for the basic events (component failure modes) analysed from field data.

Table 7.10 Failure Rate of Failure Causes

Subsystem Failure Mode	Component Failure Mode		Failure rate	Basic Event
AF function loss (A_1)	Air filter leakage		2.2×10^{-6}	X_1
	Automatic drain valve fail		1.8×10^{-6}	X_2
LV sensing error (A_2)	LV pressure change		2.0×10^{-6}	X_3
	LV short		2.2×10^{-6}	X_4
PSU sensing error (A_3)	PSU sensing error		3.0×10^{-6}	X_5
	PSU short		2.8×10^{-6}	X_6
ECU function error (A_4)	ECU in/output fail		2.3×10^{-6}	X_7
	Communication error		4.6×10^{-6}	X_8
	Power supply error		2.3×10^{-6}	X_9
EPV function error (A_5)	Automatic drain valve failed		1.8×10^{-6}	X_2
	Pressure sensing error		5.8×10^{-6}	X_{10}
	Communication error		4.6×10^{-6}	X_8
	EPV operation error (A_6)	Dregs in EPV	4.0×10^{-6}	X_{11}
		EPV leakage	5.4×10^{-6}	X_{12}

(1) Top Event (System Level):

$$F(T) = 1 - \{1 - F(A_1)\} \cdot \{1 - F(A_2)\} \cdot \{1 - F(A_3)\} \cdot \{1 - F(A_4)\}$$

$$\cdot \{1 - F(A_5)\} \qquad (7.9)$$

$$= 1 - \{1 - 4 \times 10^{-6}\} \times \{1 - 4.4 \times 10^{-12}\} \times \{1 - 8.4 \times 10^{-12}\}$$

$$\times \{1 - 9.2 \times 10^{-6}\} \cdot \{1 - 5.08 \times 10^{-6}\}$$

$$= 1.9 \times 10^{-5}$$

(2) Intermediate event (Subsystem Level)

$$F(A_1) = 1 - \{1 - F(X_1)\} \cdot \{1 - F(X_2)\} \qquad (7.10)$$

$$= 1 - \{1 - 2.2 \times 10^{-6}\} \cdot \{1 - 1.8 \times 10^{-6}\}$$

$$= 4.00 \times 10^{-6}$$

$$F(A_2) = F(X_3) \cdot F(X_4) \qquad (7.11)$$

$$= 2.0 \times 10^{-6} \times 2.2 \times 10^{-6}$$

$$= 4.40 \times 10^{-12}$$

$$F(A_3) = F(X_5) \cdot F(X_6) \qquad (7.12)$$

$$= 3.0 \times 10^{-6} \times 2.8 \times 10^{-6}$$

$$= 8.40 \times 10^{-12}$$

$$F(A_4) = 1 - \{1 - F(X_7)\} \cdot \{1 - F(X_8)\} \cdot \{1 - F(X_9)\} \qquad (7.13)$$

$$= 1 - \{1 - 2.3 \times 10^{-6}\} \times \{1 - 4.6 \times 10^{-6}\} \times \{1 - 2.3 \times 10^{-6}\}$$

$$= 9.20 \times 10^{-6}$$

$$F(A_5) = 1 - \{1 - F(X_{10})\} \cdot \{1 - F(X_6)\} \tag{7.14}$$

$$= 1 - \{1 - 5.8 \times 10^{-6}\} \times \{1 - 2.16 \times 10^{-11}\}$$

$$= 5.08 \times 10^{-6}$$

$$F(A_6) = F(X_{11}) \cdot F(X_{12}) \tag{7.15}$$

$$= 4.0 \times 10^{-6} \times 5.4 \times 10^{-6}$$

$$= 2.16 \times 10^{-11}$$

Table 7.11 shows the quantitative analysis results of the minimal cut sets.

Table 7.11 Failure Rate of Pneumatic Braking Unit

Failure Event		Frequency Level	Remark
		Failure Rate	
System Level	*F(T)*	1.90 X 10^{-05}	
Subsystem Level	*F(A$_1$)*	4.00 X 10^{-06}	
	F(A$_2$)	4.40 X 10^{-12}	
	F(A$_3$)	8.40 X 10^{-12}	
	F(A$_4$)	9.20 X 10^{-06}	
	F(A$_5$)	5.08 X 10^{-06}	
	F(A$_6$)	2.16 X 10^{-11}	

7.3.5 Risk Evaluation

This step evaluates the level of the failure severity and frequency of failure consequence by FMEA and FTA analysis, and then it determines the risk level. Table 7.12 describes the risk level of the component level of PBU.

Table 7.12 Risk Level of PBU Components

Failure Code	Component Failure Rate	Failure Frequency Level	Failure Severity Level	Risk Level
P-1	2.2×10^{-6}	3	2	2
P-2	1.8×10^{-6}	3	2	2
P-3	2.0×10^{-6}	3	2	2
P-4	2.2×10^{-6}	3	2	2
P-5	3.0×10^{-6}	3	2	2
P-6	2.8×10^{-6}	3	2	2
P-7	2.3×10^{-6}	3	3	3
P-8	4.6×10^{-6}	3	3	3
P-9	2.3×10^{-6}	3	3	3
P-10	4.0×10^{-6}	3	2	2
P-11	2.2×10^{-6}	3	2	2
P-12	1.8×10^{-6}	3	3	3

7. 4 Analysed Results

7.4.1 Risk Assessment

By the definition of railway risk, FMEA-FTA based risk assessment was used for two parameters: failure severity of failure consequence and its frequency. In this work, the failure severity levels were estimated by the engineering judgement for FMEA analysis results and the failure frequency levels were evaluated by FTA using Boolean algebra rule and the failure rate of the data collected from the field.

The risk assessment results of the PBU components produced by FMEA-FTA are enumerated in Table 7.12. In this table, the risk level values have been computed by the combination of the failure severity and its frequency level. The failure frequency level of all components revealed level 3 (remote level) although they are different values to each other. The failure severity was evaluated as level 2 or 3. The failure consequences related to AF, LV and PSU were evaluated as level 2 (marginal level) because they affect the functional reduction of PBU. The failure consequences of ECU and EPV were evaluated as level 3 (critical level) which causes the complete functional loss. Accordingly, the overall risk level of the PBU components is revealed as level 2.

Table 7.13 represents the risk level of the PBU subsystems. The FMEA-FTA risk assessment method can obtain the risk level simply. In the table, the failure frequency of LV and PSU is evaluated as Level 1 by very low failure rate, and their failure severities are estimated as level 2. Therefore, the risk level of the LV and PSU are estimated as Level 1. The ECU and EPV are revealed the level 3 in the frequency and severity; accordingly, the risk level of ECU and EPV is estimated as level 3. Finally, the risk level of AF is evaluated as Level 2. Therefore, the overall risk level of PBU subsystems is revealed as Level 2.

Table 7.14 represents the risk level of PBU in the system level, which represents level 2 by the failure frequency of Level 2 and the failure severity of Level 3. Therefore, it can be confirmed that the PBU was designed within a tolerable level.

Table 7.13 Risk Level of PBU Subsystems

Failure Code	Failure Rate	Failure Frequency Level	Failure Severity Level	Risk Level
AF	$4.00 \text{ X } 10^{-06}$	3	2	2
LV	$4.40 \text{ X } 10^{-12}$	1	2	1
PSU	$8.40 \text{ X } 10^{-12}$	1	2	1
ECU	$9.20 \text{ X } 10^{-06}$	3	3	3
EPV	$5.08 \text{ X } 10^{-06}$	3	3	3

Table 7.14 Risk Level of PBU

Failure Code	Failure Rate	Failure Frequency Level	Failure Severity Level	Risk Level
PBU	$1.90 \text{ X } 10^{-05}$	2	3	2

7.4.2 Reliability Performance Assessment

In this case study, the operational reliability performance of PBU was identified as shown in Table 7.15. The reliability performance, mean time between failures (*MTBF*), can be identified by Equation 7.16. Table 7.15 includes the result of this case study. In this analysis, the operational reliability performance was evaluated as about 52,632 *km* (1,754 *hours*) and it was confirmed as an excellent performance, compared with that of a similar system, shown in Table 7.16:

$$MTBF = \frac{1}{\lambda} = \frac{1}{F(T)} \tag{7.16}$$

$$= \frac{1}{0.000019} = 52{,}632\ km$$

$$= \frac{52{,}632}{30} = 1{,}754\ hours$$

Table 7.15 Reliability Performance of PBU

Subsystem	MTBF (hours)	MKBF (km)	Failure Rate	Remark
Braking System	1,754	52,632	0.000019	

Table 7.16 Reliability performance of Similar PBU

Subsystem	MTBF (hours)	MKBF (km)	Remark
Braking System	898	26,940	

7.4.3 Failure Analysis

The major failure causes and failure rate of PBU were identified in this case study. The failures of the system level had five different failure modes, which were generated by 12 different failure causes as described in Table 7.7. Failure rate of the components level was investigated as the range of 10^{-6} as described in Table 7.10 and it was the ‘remote level’ that was likely to occur sometimes in the life cycle. The failure rate of the subsystem level was recorded in the range of 10^{-12}< to ≤ 10^{-6} as described in Table 7.11 and it was the ‘remote or impossible level’ that was likely to occur sometimes in the life cycle or it is unlikely to occur. The failure rate of the system level was investigated as the range of 10^{-5} as described in Table 7.11 and it was the ‘occasional level’ that was likely to occur several times.

In the fault tree analysis, all subsystems of the PBU were connected by OR gate. Accordingly, any failure amongst all subsystems directly affects the function of PBU. The PBU has six single point failures that directly affect the top event as shown in Table 7.17. These single point events also require specific maintenance actions to keep their functions.

Table 7.17 Single Point Failures of PBU

Category	Minimal Cut Sets	Set
1 MCS for basic event	(X_1), (X_2), (X_7), (X_8), (X_9), (X_{10})	6

In conclusion, the case study has been applied to a very small safety unit due to the lack of system description, information and data available and experience, but the risk level, failure rate and single point failures are effectively identified.

7.5 Summary

This chapter has performed the risk assessment of the existing pneumatic braking unit of railway vehicle as a case study, which is conducted to demonstrate how the proposed risk assessment methods based on FMEA-FTA technique can be used to analyse and evaluate their risk level, and confirm the reliability performance level. The FMEA-FTA risk assessment offers a great potential in the systems design analysis and their risk assessment, especially in assessing the uncertainty level of railway systems related to high safety.

Railway risk assessment using FMEA-FTA techniques allows the flexibility for the information and data available and the systems design phase applied, by the application of qualitative, semi-quantitative and quantitative risk assessment and top-down and bottom-up approach. In addition, the flexibility encourages the use of information and data from various sources such as qualitative descriptions, engineering judgement and the various combinations of typical risk techniques such as ETA, HAZOP and fishbone diagram etc.

However, this case study was used for the product design phase without the design performance criteria. In the case assessment, the risk level of all system levels were assessed as the acceptance level, but the data and information management appropriate to risk assessment is required to introduce RAMS management effectively.

Chapter 8

CONCLUSIONS AND RECOMMENDATIONS

8.1 Conclusions

This research project has achieved the objectives which were planned to achieve the successful integration of RAMS management into railway systems engineering by developing several models and processes, and providing possible techniques that are applicable to RAMS management. This research has proved that the proposed management models, processes and techniques can help railway organisations establish and implement RAMS management at the system concept design phase. The major achievements of the research can be summarised as follows:

This research has firstly achieved the objective of establishing the theoretical engineering background associated with systems RAMS management. The systems RAMS management is a branch management discipline of systems engineering. Thus, this research defined the concepts of systems engineering to provide a fundamental basis for the overall functions and life cycle activities of RAMS management. This research established the concept of systems RAMS management in three aspects: (1) the definition of RAMS characteristics appropriate to the operational requirements, (2) the provision of the means to prevent railway RAMS risks, and (3) the assessment and control of all potential hazards threatening the operational requirements. This research established risk assessment methods in the two aspects: (1) top-down and bottom-up approach and (2) qualitative, quantitative, and/or combined semi-approach. The typical risk assessment techniques, such as PHA, FMEA, FTA etc., were briefly investigated for their objectives, advantages, disadvantages, etc. to consider their application for the railway risk assessment process. These outcomes have been achieved through an extensive review of diverse literature. Through these literature reviews, three approaches for the railway RAMS management were established: risk based RAMS management, systems based RAMS management and life cycle based RAMS management.

Recent global railway projects have required the implementation of RAMS management to achieve a railway traffic service safely within the defined time and limited cost. Thus, it becomes a key issue to think of integrating RAMS management into railway systems engineering. Accordingly, this research has secondly achieved the objective of developing the systematic approach method of RAMS management for railway systems engineering to integrate the RAMS management into railway systems engineering effectively. This research proposed railway RAMS management systems approach for the successful integration of the RAMS management. This research established railway systems engineering process and its process activities through several process models to provide a fundamental basis of the process, functions, activities and techniques related to RAMS management. This research also established the risk based railway RAMS management process to focus the RAMS management on assessing and controlling all railway RAMS risks. The proposed RAMS management systems, railway systems engineering process and risk based RAMS management process will be essential elements to implement RAMS management in the railway engineering project.

Railway risks have a great potential to cause injury and/or loss of the life of staffs or passengers, the environmental degradation, damage to property and adverse impact in the railway operational contexts. Thus, the assessment and control of railway risks is the major focus of railway RAMS management. Accordingly, this research has thirdly achieved the objective of developing the methods that assess all railway hazards affecting the railway traffic service, based on the combination of FMEA-FTA technique. This research provided FMEA-FTA based railway risks assessment models that are applicable to each system engineering design phase: the top-down approach model for the risk assessment of the functional architecture, and the bottom-up approach model for the risk assessment of the design architecture. This research provided FMEA-FTA based railway risk assessment process model that can be applied to all system design phases. The risk assessment process includes the development of risk scenario through FMEA, fishbone diagram, ETA and FTA; the qualitative assessment of the failure cause scenario through the minimal cuts analysis and Boolean algebra rules; and the quantitative assessment of the risk scenarios through the failure probability or failure rate. The proposed FMEA-FTA risk assessment technique has a great potential to assess safety, availability, reliability and maintainability. Accordingly, the FMEA-FTA combination models are very useful to the risk assessment of the railway system as well as the mission and safety critical system.

Specifying RAMS requirements and operational contexts is a fundamental basis of RAMS management to provide the RAMS design solutions and their acceptance performance criteria. Thus, it requires the systematic and quantitative RAMS requirements to the customers and it also requires the successful RAMS performance specification process activities to the suppliers. Accordingly, this research has fourthly achieved the objective of developing the methods that specify RAMS requirements and operational contexts to provide RAMS design solutions and their acceptance performance criteria and to facilitate the system design efforts and contract. For this purpose, this research provides a framework that implements railway RAMS performance specification. The framework provides several methods such as the establishment of the railway service objectives, the definition of railway RAMS concept, the definition of RAMS performance specification principle, and the selection of RAMS measures needed. This research provides a RAMS performance specification process that is applicable to all different design phases. The specification process provides the process activities and techniques such as the determination of railway service performance and measures; the determination of operational RAMS effectiveness; the assessment of operational behaviours; the RAMS performance trade-off/control; RAMS performance allocation; and RAMS performance verification.

This research has finally achieved the objective of conducting a case study on the proposed railway risk assessment to demonstrate the proposed FMEA-FTA based risk assessment method and to confirm the RAMS performance level and major failures of the existing pneumatic braking unit. In the case study, the detailed structural and functional descriptions for pneumatic braking unit were described to analyse all possible failures. The analysed failures were compared with the failure data collected from the field to determine the failure consequences. The risk parameters, risk levels and risk evaluation matrix were established through the analysis results of the field data. The major failure consequences that affect the full service braking function were analysed for their severity and the causes of the failure consequences were also analysed by the fault tree construction, and minimal cut set analysis by using the Boolean algebra rule.

The proposed RAMS models, processes, and techniques have attracted the high levels of interest from the railway industry. These research results will be a cornerstone for the introduction of railway RAMS management and they have a significant influence on the introduction of RAMS management to many railway organisations.

8.2 Recommendations for further work

The proposed models, processes and techniques have been designed and developed to provide the systematic approach of RAMS management for railway systems engineering. They will facilitate and encourage railway organisations in establishing and introducing RAMS management. However, as for any other research, it is necessary to provide recommendations for further improvement and upgrade of the proposed models, processes, and techniques associated with railway RAMS management, in order to allow the introduction and continuous improvement of the application of RAMS management to railway organisations.

The results of this research project will be a solid cornerstone for further development and modification of the models, processes, and techniques related to railway RAMS management, so that they are applicable to many railway fields more efficiently and effectively. More efforts should be undertaken to enhance the awareness of RAMS management in the railway industry to integrate RAMS management into railway systems engineering, and more engineering techniques should be developed to support railway systems engineering effectively.

REFERENCES:

Ahmad, H. S. M. (2011). **Development of KM model for knowledge management implementation and application in construction projects**. PhD, University of Birmingham.

An, M., Wright, I., Foyer, P. & Lupton, J. (2002). **Safety Assessment in Railway-The current Status and Future Aspects.** *In:* Proceedings of the International Conference Railway Engineering 2002, held London, UK, July 2002-CD ROM, 2002.

An, M, Huang. S & C. Baker (2004). **Safety management in the UK railway network.** Proceedings of the 6th International Railway Engineering (CD format), Engineering Technics Press Edinburgh, London, UK.

An, M. (2005). **A review of design and maintenance for railway safety - the current status and future aspects in the UK railway industry**. World Journal of Engineering, Vol.2 (3)**,** pp.10-22.

An, M. Chris, B & Zeng, J (2005). **A fuzzy-logic-based approach to qualitative risk modelling in the construction process**. World Journal of Engineering, Vol.2 (3)**,** pp.10-22.

An, M., Lin, W. & Stirling, A. (2006). **Fuzzy-reasoning-based approach to qualitative railway risk assessment**. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, Vol.220**,** pp.153-167.

An, M. Huang, S & Baker, C.J (2007). **A railway risk management - The fuzzy reasoning approach and fuzzy-analytical hierarchy process approaches: a case study.** Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, Vol.221**,** pp.1-19.

An, M., Chen, Y. & Baker, C. J. (2011). **A fuzzy reasoning and fuzzy-analytical hierarchy process based approach to the process of railway risk information: A railway risk management system**. Information Sciences, Vol.181**,** pp.3946-3966.

Andrews, J. (2012). **Introduction to Fault Tree Analysis**. *In:* 2012 Annual RELIABILITY and MAINTAINABILITY Symposium, 2012.

EIA (1994). **EIA/IS-632**. EIA Interim Standard, Engineering Department, Washington, DC.

Berrado, A., El-Koursi, E., Cherkaoui, A. & Khaddour, M. (2010). **A Framework for Risk Management in Railway Sector: Application to Road-Rail Level Crossings**. Open Transportation Journal.

Bertalanffy, L. V. (1968). VON (1968):"**General Systems Theory"**. New York: George Braziller.

Bitsch, F. (2003). **Process Model for the Development of System Requirements Specifications for Railway Systems**.

Blanchard, B. S. (2012). **System engineering management**, Wiley.

Blanchard, B. S., Fabrycky, W. J. & Fabrycky, W. J. (1990). **Systems engineering and analysis**, Prentice Hall Englewood Cliffs, New Jersey.

Blanchard, B. S., Verma, D. A. & Peterson, E. L. (1995). **Maintainability: A key to effective serviceability and maintenance management**, Wiley-Interscience.

Bonnett, C. F. (2005). **Practical railway engineering**, World Scientific.

Braband, J., Hirao, Y. & Luedeke, J. F. (2003). **The Relationship between the CENELEC Railway Signalling Standards and Other Safety Standards**. Signal und Draht, Vol.95**,** pp.32-38.

Breemer, J. (2009). **RAMS and LCC in the design process of infrastructural construction projects: an implementation case**.

Bryman, A. & Bell, E. (2007). **Business research methods**, Oxford University Press, USA.

BS EN 31010 (2008). **Risk Management – Risk Assessment Techniques**. London: British Standards Institution (BSI).

BS EN 50126-1 (1999). **Railway applications – The Specification and Demonstration Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic Requirements and Generic Process**. London: British Standards Institution (BSI).

BS EN 50126-2 (2007). **Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 3: Guide to the Application of EN 50126-1 for Safety**. London: British Standards Institution (BSI).

BS EN 50126-3 (2006). **Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 3: Guide to the application of EN 50126-1 for Rolling Stock RAMS**. London: British Standards Institution (BSI).

BS EN 50128 (2009). **Railway Applications - Communication, Signalling and Processing Systems - Software for Railway Control and Protection Systems**. London: British Standards Institution (BSI).

BS EN 50129 (2003). **Railway Applications - Communication, Signalling and Processing Systems - Safety related Electronic Systems for Signalling**. London: British Standards Institution (BSI).

BS EN 60300-3-1 (2004). **Dependability Management – Part 3-1: Analysis Techniques for Dependability – Guide on Methodology**. London: British Standards Institution (BSI).

BS EN 60300-3-2 (2004). **Dependability Management – Part 2: Guidelines for dependability management**. London: British Standards Institution (BSI).

BS EN 60300-3-4 (2004). **Dependability Management –** Part 3-4: Application guide — Guide to the specification of dependability requirements. London: British Standards Institution (BSI).

BS EN 60300-3-5 (2008). **Dependability Management – Part 3-5: Application guide — Reliability test conditions and statistical test principles**. London: British Standards Institution (BSI).

BS-EN 60300-3-11 (2009). **Dependability Management – Part 3-11: Application Guide – Reliability Centred Maintenance**. London: British Standards Institution (BSI).

BS EN 60300-3-15 (2007). **Dependability management - Part 3-15: Guidance to engineering of system dependability**. London: British Standards Institution (BSI).

BS EN 60812 (2006). **Analysis Techniques for System Reliability – Procedure for Failure Mode and Effects Analysis (FMEA)**. London: British Standards Institution (BSI).

BS EN 61025 (2007). **Fault tree analysis (FTA)**. London: British Standards Institution (BSI).

BS EN 61078 (1994). **Reliability of Systems, Equipment and Components —Part 9: Guide to the block diagram technique**. London: British Standards Institution (BSI).

BS EN 61124 (2006). **Reliability testing - Compliance tests for constant failure rate and constant failure intensity**. London: British Standards Institution (BSI).

BS EN 61164 (2004). **Reliability Growth - Statistical test and estimation methods**. London: British Standards Institution (BSI).

BS EN 61508-1~7 (2002, 2005). **Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1 to 7: Functional safety and IEC 61508**. London: British Standard Institution (BSI).

BS EN 62347 (2007). **Guidance on system dependability specifications**. London: British Standards Institution (BSI).

BS EN 62502 (2009). **Analysis techniques for dependability Event Tree Analysis**. London: British Standards Institution (BSI).

BS IEC 706-3 (2006). **Maintainability of equipment - Part 3: Guide to maintainability verification, and the collection, analysis and presentation of maintainability data**. London: British Standards Institution (BSI).

BS IEC 60300-3-5 (2001). **Part 3-5: Application guide - Reliability test conditions and statistical test principles**. London: British Standards Institution (BSI).

BS IEC 60300-3-10 (2001). **Dependability management - Part 3-10: Application guide - Maintainability**. London: British Standards Institution (BSI).

BS IEC 61882 (2001). **Hazard and Operability studies (HAZOP studies – Application guide**. London: British Standards Institution (BSI).

BS IEC 62198 (2001). **Project Risk Management – Application Guidelines**. London: British Standards Institution (BSI).

BS ISO 9000 (2005). **Quality Management Systems – Fundamentals and Vocabulary**. London: British Standards Institution (BSI).

BS ISO 9001 (2005). **Quality Management Systems – Requirements**. London: British Standards Institution (BSI).

BS ISO 13824 (2008). **General principles on risk assessment of systems involving structures**. Lodon: British Standards Institution (BSI).

BS ISO 15288 (2002). **Systems Engineering – System Life cycle Processes**. Lodon: British Standards Institution (BSI).

BS ISO/IEC 26702 (2007). **Systems Engineering – Application & Management of the Systems Engineering Process**. London: British Standards Institution (BSI)

C. Haskins, K. F. a. M. K. (2007). **Systems Engineering Handbook: A Guide for System Life Cycle Process and Activities**. International Council on Systems Engineering (INCOSE).

Cantos, P. & Campos, J. (2005). **Recent changes in the global rail industry: facing the challenge of increased flexibility**.

Carretero, J., Pérez, J. M., García-Carballeira, F., Calderón, A., Fernández, J., GarcíA, J. D., Lozano, A., Cardona, L., Cotaina, N. & Prete, P. (2003). **Applying RCM in large scale systems: a case study with railway networks**. Reliability Engineering & System Safety, Vol.82**,** pp.257-273.

Cha, J. (2010). **Study on the Improvement of Preventive-Maintenance on Pneumatic Braking System using FMECA**. Seoul National University of Science & Technology.

Chen, Y. (2012). **Improving Railway Safety Risk Assessment Study**. PhD, University of Birmingham.

Choi, J. (2008). **Risk Matrix and PHA Development of Rolling Stock - Final Report on Risk Matrix and PHA Development of Rolling Stock for KORAIL.** Korea: LIoyd's Register.

Clark, J. O. (2008). **System of systems engineering and family of systems engineering from a standards perspective**. *In:* System of Systems Engineering, 2008. SoSE'08. IEEE International Conference on, 2008. IEEE, 1-6.

Daup (2001). **Systems Engineering Fundamentals**, Vergina, USA, Defense Acquisition University Press.

Despotou, G. (2007). **Managing the Evolution of Dependability Cases for Systems of Systems**, University of York, Department of Computer Science.

Ebeling, C. E. (2010). **An Introduction to Reliability and Maintainability Engineering**, Canada, Waveland Press, Inc.

El-Koursi, E., Mitra, S. & Bearfield, G. (2007). **Harmonising safety management systems in the European railway sector**. Safety Science Monitor, Vol.11.

Elphick, J. (2010). **Railway Systems Engineering Why is Water Wet?** *In:* Railway Signalling and Control Systems (RSCS 2010), IET Professional Development Course on, 2010. IET, 250-270.

Ericson, C. A. (1999). **Fault Tree Analysis – A History** *In:* Proceeding of the 17th International System Safety Conference 1999 1999.

Ericson, C. A. (2005). **Hazard analysis techniques for system safety**, Wiley-Interscience.

ERTMS (1998). **ETCS RAMS Requirements Specification**. Ref. 96s1266.

Fiet, J. E. (2010). **RAILWAY SYSTEMS ENGINEERING**.

Gofuku, A., Koide, S. & Shimada, N. (2006). **Fault tree analysis and failure mode effects analysis based on multi-level flow modeling and causality estimation**. *In:* SICE-ICASE, 2006. International Joint Conference, 2006. IEEE, 497-500.

Gorod, A., Sauser, B. & Boardman, J. (2008). **System-of-systems engineering management: a review of modern history and a path forward**. Systems Journal, IEEE, Vol.2**,** pp.484-499.

Green, J. M. (2001). **Establishing system measures of effectiveness**. DTIC Document.

Ho, C. (2008). **Effective application of systems assurance techniques on complex railway development projects**. *In:* Railway Engineering-Challenges for Railway Transportation in Information Age, 2008. ICRE 2008. International Conference on, 2008. IET, 1-10.

Hokstad, P., Dg, E., Sintef, L., Øien, K. & Vatn, J. (1998). **Life Cycle Cost Analysis in Railway Systems**. SINTEF Safety and Reliability.

Hwang, J.-G. & Jo, H.-J. (2008). **RAMS management and assessment of railway signaling system through RAM and safety activities**. *In:* Control, Automation and Systems, 2008. ICCAS 2008. International Conference on, 2008. IEEE, 892-895.

IEC (2009). **Concept of Dependability**. IEC TC56 WG3 Dependability Management

Jenkins, G. & Youle, P. (1968). **A systems approach to management**. OR**,** pp.5-21.

Jung, E.-J., Oh, S.-C., Park, S.-H. & Kim, G.-D. (2009). **Safety criteria and development methodology for the safety critical railway software.** *In:* Telecommunications Energy Conference, 2009. INTELEC 2009. 31st International, 2009. IEEE, 1-4.

Ju, H., Xiang, W., Lu, Y. & Du, X. (2011). **Integrating RAMS approach on the safety life cycle of rail transit**. *In:* Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2011 International Conference on, 2011. IEEE, 801-803.

Jung, I, S (2009). **Study on the Setting-up & Demonstration of RAMS requirements in Rolling Stock**. Seoul National University of Science and Technology

Jung,W. Kim, H. & Yoo, J (2001). **A Classification and Selection of Reliability Growth Models.** University of Daegu

Kapurch, S. J. (2010). **NASA Systems Engineering Handbook**, DIANE Publishing.

Kaufmann, J. J. (1982). **Function analysis system technique (FAST) for management applications**. Value World, Vol.5.

Kendall, K. E., Kendall, J. E., Kendall, E. J. & Kendall, J. A. (1992). **Systems analysis and design**, Prentice Hall Englewood Cliffs.

Kennedy, A. (1997). **Risk management and assessment for rolling stock safety cases**. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, Vol.211**,** pp.67-72.

Khisty, C. J. & Mohammadi, J. (2002). **Fundamentals of Systems Engineering**. IIE Transactions, Vol.34**,** pp.329ą333.

Kim, J. (2008). **The Study on FTA of Full Service Brake Equipments for Making Safety about Rolling Stock System**. Korea: Seoul National University of Science & Technology.

Kim, J., Jeong, H. & Park, J. (2009). **Development of the FMECA process and analysis methodology for railroad systems**. International Journal of Automotive Technology, Vol.10**,** pp.753-759.

Kossiakoff, A., Sweet, W. N., Seymour, S. & Biemer, S. M. (2011). **Systems engineering principles and practice**, Wiley-Interscience.

Krri (2007). **Basic Studies for Construction of Reliability, Availability and Maintainability Management System for Railway System**. Korea: Korean Railway Reserach Institution.

Li, Y. H., Wang, Y. D. & Zhao, W.-Z. (2009). **Bogie failure mode analysis for railway freight car based on FMECA**. *In:* Reliability, Maintainability and Safety, 2009. ICRMS 2009. 8th International Conference on, 2009. IEEE, 5-8.

Lundteigen, M. A., Rausand, M. & Utne, I. B. (2009). **Integrating RAMS engineering and management with the safety life cycle of IEC 61508**. Reliability Engineering & System Safety, Vol.94**,** pp.1894-1903.

Lyngby, N., Hokstad, P. & Vatn, J. 2008. **RAMS management of railway tracks**. *Handbook of performability engineering.* Springer.

Markeset, T. & Kumar, U. (2003). **Integration of RAMS and risk analysis in product design and development work processes: a case study**. Journal of Quality in Maintenance Engineering, Vol.9**,** pp.393-410.

Martin, J. N. (1998). **Overview of the EIA 632 standard- Processes for engineering a system**. *In:* DASC- AIAA/IEEE/SAE Digital Avionics Systems Conference, 17 th, Bellevue, WA, 1998.

Mil Hdbk 189c (2011). **Handbook of Reliability Growth Management**. Washington DC: Department of Defense.

Mil Hdbk 388b (1998). **Military Handbook - Electronic Reliability Design Handbook**. Washington DC: Department of Defense.

Mil Hdbk 470a (1997). **Department of Defense Handbook - Designing and developing Maintenance products and systems** Washington, SC: Department of Defense.

Mil Hdbk 781a (1996). **Handbook for Reliability Test Methods, Plans, and Environments for Engineering, Development Qualification and Production**. Washington, DC: Department of Defense.

Mil Std 499 (1969). **Engineering Management**. Washington, DC: Department of Defense.

Mil Std 499a (1974). **Engineering Management**. Washington, DC: Department of Defense.

Mil Std 499b (1994). **Systems Engineering (Draft)**. Washington, DC: Military Standard, Notice 1, DoD.

Mil Std 882d (2000). **Standard Practice for System Safety**. Washington, DC: Department of Defense, DoD.

Mil Std 1629a (1980). **Procedures for performing a Failure Mode, Effect and Criticality Analysis**. Washington, DC: Department of Defense, DoD.

Milutinović, D. & Lučanin, V. (2005). **Relation between reliability and availability of railway vehicles**. FME Transactions, Vol.33**,** pp.135-139.

Morfis, M. (2009). **Illustrating the benefits of systems engineering in railways: case study in London Underground**.

Moubray, J. (2001). **RCM II: reliability-centered maintenance**, Industrial Press Inc.

Muttram, R. (2002). **Railway safety's safety risk model**. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, Vol.216**,** pp.71-79.

Nicholls, D. (2005). **System Reliability Toolkit**, Riac.

Niels Peter Hoj, W. K. (2002). **Risk analysis of transportation on road and railway from a European Perspective**. SAFETY SCIENCE**,** pp.337-357.

Nordland, O. (2003). **A critical look at the cenelec railway application standards**.

P. Valkokari, T. A., O. Venho-Ahonen, H. Franssila and A. Ellman (2012). **Requirements for Dependability Manangement and ICT Tools in the Early Stages of the System Design**. Adance in Safety, Reliability and Risk Manangement. 2012 Taylor & Francis Group.

Pan, H., Tu, J., Zhang, X. & Dong, D. (2011). **The FTA based safety analysis method for urban transit signal system**. *In:* Reliability, Maintainability and Safety (ICRMS), 2011 9th International Conference on, 2011. IEEE, 527-532.

Puntis, R. & Walley, D. (1986). **The use of reliability techniques on traction and rolling stock**. Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering, Vol.200**,** pp.295-304.

Papadopoulos, Y., Walker, M., Parker, D., Rüde, E., Hamann, R., Uhlig, A., Grätz, U. & Lien, R. (2011). **Engineering failure analysis and design optimisation with HiP-HOPS**. Engineering Failure Analysis, Vol.18**,** pp.590-608.

Pasquale, T., Rosaria, E., Pietro, M., Antonio, O. & Segnalamento Ferroviario, A. (2003). **Hazard analysis of complex distributed railway systems**. *In:* Reliable Distributed Systems, 2003. Proceedings. 22nd International Symposium on, 2003. IEEE, 283-292.

Profillidis, V. A. (2007). **Railway management and engineering**, Ashgate Publishing, Ltd.

Rafrafi, M., Bourdeaud'huy, T. & El Koursi, E. (2006). **Risk Apportionment Methodology Based On Functional Analysis**. *In:* Computational Engineering in Systems Applications, IMACS Multiconference on, 2006. IEEE, 1103-1109.

Robert Bogovini, S. P. a. M. R. (1993). **Failure Mode, Effects and Criticality Analysis**. New York: Reliability Analysis Center.

Rooney, A. & Pretorius, L. (2001). **A Management Approach to Reliability Growth for Complexelectromechnical Systems**. South African Journal of Industrial Engineering, Vol.12.

Rotem (2007). **RAMS Plan (Reliability, Availability, Maintainability and Safety Plan).** KII-1-E3100-P-001. REDE 100051.

Sage, A. P. (1995). **Risk management systems engineering**. *In:* Systems, Man and Cybernetics, 1995. Intelligent Systems for the 21st Century., IEEE International Conference on, 1995. IEEE, 1033-1038.

Sage, A. P. & Rouse, W. B. (2011). **Handbook of systems engineering and management**, Wiley-Interscience.

Schäbe, H. (2001). **Different approaches for determination of tolerable hazard rates**. *In:* ESREL, 2001. 435-442.

Seong-Phil Eo, S.-J. K. a. D.-Y. K. (2010). **Establishing RAM Requirement based on BCS model for weapon Systems**. Korean Weapon Technical Institution, Vol.1**,** pp.67-76.

Sheard, S. A. (2001). **Evolution of the frameworks quagmire**. Computer, Vol.34**,** pp.96-98.

Shenhar, A. (1994). **Systems engineering management: a framework for the development of a multidisciplinary discipline**. Systems, Man and Cybernetics, IEEE Transactions on, Vol.24**,** pp.327-332.

Smith, S. A. & Oren, S. S. (1980). **Reliability growth of repairable systems**. Naval Research Logistics Quarterly, Vol.27**,** pp.539-547.

Stamatelatos, M. & Caraballo, J. (2002). **Fault tree handbook with aerospace applications**, Office of safety and mission assurance NASA headquarters.

Stapelberg, R. F. (2008). **Handbook of reliability, availability, maintainability and safety in engineering design**, Springer.

Sutherland. G (2004). **KRRI RAMS Trainning Final Report**. Korean Railroad Research Institute.

Tatry, P., Deneu, F. & Simonotti, J. (1997). **RAMS approach for reusable launch vehicle advanced studies**. Acta astronautica, Vol.41**,** pp.791-797.

Ting, T., Yue, L., Tao-Tao, Z., Hai-Long, J. & Hai, S. (2011). FTA and FMEA of braking system based on relex 2009. *In:* Information Systems for Crisis Response and Management (ISCRAM), 2011 International Conference on, 2011. IEEE, 106-112.

Ucla, A. A., Avizienis, A., Laprie, J.-C. & Randell, B. (2001). **Fundamental concepts of dependability**.

Umar, A. A. (2010). **Design for safety framework for offshore oil and gas platforms**. University of Birmingham

Villemeur, A. (1992). **Reliability, Availability, Maintainability and Safety Assessment: Volume 1 - Methods and Techniques**. Chicester, England: John Wiley & Sons.

Vintr, Z. & Vintr, M. **Reliability and Safety of Rail Vehicle Electromechanical Systems**.

Vintr, Z. & Vintr, M. (2007). **RAMS program for electromechanical systems of railway applications**.

Wengong, W., Liyun, D., Ping, J. & Jun, W. (2008). **The Planning and Application of RAMS Specifications in Urban Rail Transit [J]**. Railway Quality Control, Vol.6**,** pp.005.

Yahiaoui, A., Sahraoui, A., Hensen, J. & Brouwer, P. (2006). **A systems engineering environment for integrated building design**. *In:* European Systems Engineering Conference (EuSEC), Edinburgh, UK, 2006.

Yu, Z., Zhao, L., Haiying, C. & Yuling, H. (2010). The study on electric-pneumatic transfer control of the train brake system. *In:* Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on, 2010. IEEE, 388-392.

Zhou, H.-L., Chang, W.-B., Zhou, S.-H. & Tan, Z.-H. (2001). Research on the converse FTA-FMECA comprehensive analysis based on Monte Carlo Simulation. *In:* Industrial Engineering and Engineering Management (IE&EM), 2011 IEEE 18Th International Conference on, 2011. IEEE, 1159-1162.

APPENDIX:

Paper Presented at International Railway Engineering Conference

London, UK

June, 2011

A METHODOLOGY FOR ROLLING STOCK RAM TARGET SETTING DEMONSTRATION

Mun Gyu Park and **Min An**
Safety and Reliability Management Research Group
School of Civil Engineering
The University of Birmingham, B15 2TT, UK
Email: m.an@bham.ac.uk

Keywords: Rolling Stock RAM, RAM Target setting up, and Service Performance

The purpose of railway rolling stock RAM (reliability, availability, and maintainability) analysis is to set up targets in order to improve service performance of rolling stock to the required level, for example, quality of service, performance of reliability and safety, and availability of equipment etc. Therefore, the quantitative targets of rolling stock RAM have to take service performance requirement into consideration and the performance of rolling stock achieved must precisely demonstrated the objective evidences that consist with service performance objectives. Although some work has been conducted in this field, no formal methodologies have been and applied to a stable environment in the railway industry. This paper presents a methodology for setting the quantitative RAM targets based on Service performance objectives, i.e. reliability, availability and maintainability of rolling stock, service pattern and maintenance resource. This paper also discusses the methods of the implementation of RAM target setting up.

INTRODUCTION

As rolling stock engineering field, reliability, availability, and maintainability (RAM) are relatively new. The application of RAM engineering to rolling stocks has been motivated by several factors such as the complexity of the system, the advance in technology, the increase of the system life cycle cost, and the change of railway management environments. RAM engineering into rolling stock is becoming a decision making factor in railway business environment because it takes a great influence on system life cycle cost and system effectiveness. Therefore, a dependable rolling stock is achieved as a result of the application of RAM engineering.

From system effectiveness perspective, RAM engineering deals with the availability performance of a rolling stock as part of system engineering and its factors affecting RAM: reliability and maintainability. The Reliability directly affects the length of a system operation. On the other hand, the maintainability is interested in decreasing the length of the system maintenance. From the cost perspective, RAM engineering has to be evaluated over the life cycle period of a system, not only initial acquisition. RAM approach for rolling stock engineering increases the cost effectiveness with the increase of the system performance.

However, when turns our rolling stock industries, many problems caused may be from the result that does not apply system engineering as well as RAM engineering. The overall system requirements for a rolling stock have been not specified from the beginning concept and design phase. The specification process of the customer requirements are relatively very short and in many cases the approach for system is firstly to finish the specification and design phase as soon as possible and the to fix it when it failed.

This paper focuses on the process and activities for specifying the established system characteristics included RAM characteristics appropriate to the operational objectives of a rolling stock. For this, the first discusses the definition of system characteristics based on system approach through the analysis of customer requirements. The next emphasises on the process activities for specifying RAM performance characteristics suitable to system objective and shows the examples specifying for RAM characteristics.

SPECIFICATION OF ROLLING STOCK

In rolling stock engineering, there are a set of engineering activities through the life cycle of the system. The specification of rolling stock is defined, as part of system engineering, as specification process activities that translate the operational objectives of a rolling stock into the system characteristics and a system configuration throughout the process of system specification; allocation; and synthesis to optimise the system design and integrate RAM characteristics into the system functions (MIL-STD-499B, 1992; MIL-HDBK-388B, 1998; Blanchard et al. 2006; EN 60300-4, 2008).

The specification of the rolling stock needs to identify in general: such as (1) the fundamental distinction of a system; (2) the system elements and the system location within the system hierarchy; (3) technology for the design of a system; (4) system complexity and scope, and the requirements; and (5) the range of system specification process; (6) system classification;

(7) RAM characteristic specification (Blanchard et al. 2006). The system specification is essential for specifying RAM characteristics. The discussion for the definition of system characteristics and influencing conditions with the definition for RAM characteristics needs.

DEFINITION OF SYSTEM CHARACTERISTICS

Customers require rolling stocks with characteristics that their system requirements are sufficiently applied. The requirements are technically characterised by the system specification process using a system approach. The process includes the definition of system characteristics into the functions needed in achieving operational objectives of the system. The outcome of the process involves the methods of system design and the demonstration criteria for the system acceptance (BS EN 60300-4, 2008). A system has a purpose and objectives to provide a focus for definition of the system characteristics.

A rolling stock is, in general, designed for a specific purpose to accomplish the operational objectives of the system. The system has general or specific objectives needed to effectively deliver the purpose which is for achievement of a defined level of rail traffic safely with railway infrastructures. The former objective includes the perception of the customer for the system quality, availability, and safety in the system perspective. The latter objective is related to the dedicated tasks, included a sequence of tasks. Accordingly, the purpose and objectives of a system becomes a framework in defining a system technically for the requirements of the customers. Defining a system is a key prerequisite to achieve the characteristics of the system (BS EN ISO 9000, 2005; Blanchard et al. 2006; BS EN 62347, 2007). System properties of a system are the features or attributes inherent of the system.

As illustrated in Figure 1, a rolling stock has a set of system properties, which are selected or assigned into the system characteristics in order for implementation of the operational objectives of the system as discussed above. These properties are used to develop the major functions needed in carrying out the tasks of the system. The specific features or attributes of a system are represented by these properties. They are categorised into property groups as shown in Figure 1. A property group has a set of system characteristics relevant to and dominant in that group.

As mentioned above, the functions of the system needed in performing the operational tasks of a rolling stock are originated from these system properties by dint of the interaction of the system elements which constitute the system. The system elements are developed to represent system characteristics to enable the functions of the system and to deliver the tasks. The system characteristics can express by quantitative or qualitative value, and they can be measured through several technical methods (Blanchard et al. 2006; BS EN 62347, 2007; Rausand, 2008). A system RAM can select as a specific system property which includes its characteristics.

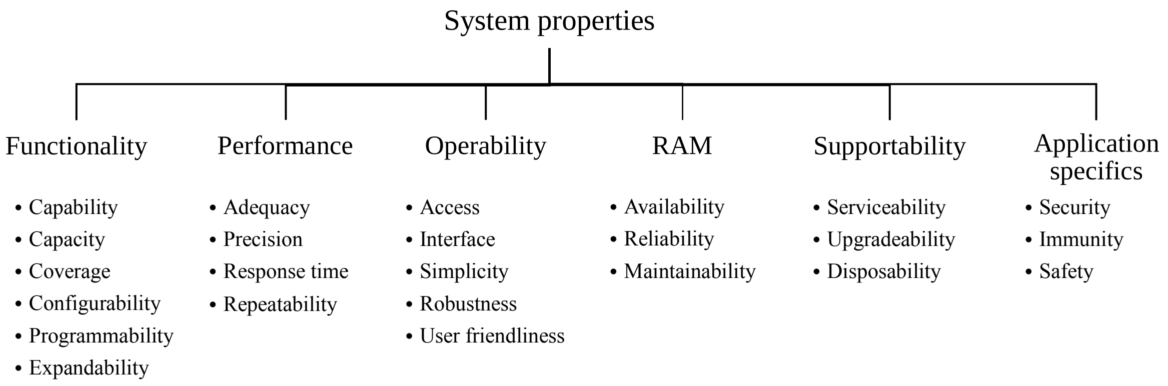


Figure 1 Examples of System Properties and Characteristics

Rolling stock RAM is the collective term for explanation of the availability performance of a rolling stock with both reliability and maintainability performance characteristics which have an influence on the availability performance. In recent rolling stock industries, these RAM characteristics have recognised as the major system performance characteristics because they take a great influence on the system effectiveness and life cycle cost. They are related to time dependent performance characteristics of the functions of the system. The availability performance represents the effectiveness of system operation, the reliability performance means the lasting of system operation without any failure; and the maintainability performance expresses the ease access for maintenance action (BS EN 60300-1, 2003; BS EN 62347, 2007).

CONDITIONS INFLUENCING SYSTEMS CHARACTERISTICS

A rolling stock, itself, cannot meet its system characteristics which enable the functions appropriate to achieving the operational objectives of the system. The system characteristics rely on the conditions such as mission profile, utilisation environments, life cycle, and maintenance concept that the system will be confronted throughout the implementation of the tasks. Therefore, it is essential to define and specify the conditions influencing prior to the definition of the system characteristics (BS EN 62347, 2007; BS EN 50126-1, 1999). The specification of affecting the conditions of a system is a process that identifies and selects the system properties and its related characteristics of the system.

The relationship between the system properties of a system and the conditions that affects them helps in identifying the conditions which influence the functions of the system. The influencing conditions are utilised to select specific system properties and related characteristics. As illustrate in Figure 2, the system characteristics selected are determined by the iterative process of the evaluation and trade-off analysis, which ultimately determine the system configuration and boundaries and form the basis for specifying the system characteristics. Each influencing conditions may be influenced by various factors: for example, the task of the system is affected by the factors such as nature, scope, duration, sequence of the task, mode of operation, operation scenario, and the system environments is influenced by the temperature and humidity (BS EN 62347, 2007; BS EN 50126-1, 1999).

ROLLING STOCK RAM SPECIFICATION PROCESS

The specification of a rolling stock can be efficiently achieved in terms of the use of a process through a system approach (BS EN ISO 9000, 2005). The process iteratively executes numerous linked specification activities to transform operational objectives into a complete system configuration under the on-going control. Accordingly, Rolling stock RAM needs the application of an integrated process approach for specifying their performance characteristics. The process aims to: (1) establish the purpose and objectives of the application of RAM; (2) determine the RAM requirements and the method for achievement of them; (3) allocate the RAM requirements towards lower systems; and (4) model and predict the RAM results performed; and make decision on the RAM results. System specification process assists in promoting the specification of RAM characteristics effectively.

ROLLING STOCK SPECIFICATION PROCESS

As mentioned above, the system specification process forms a framework for the broad application of engineering activities for RAM characteristics. It provides guidance on the RAM specification during the design phase of the system life cycle. Figure 2 describes a framework model for specifying system characteristics. The development of a process appropriate to system characteristics is necessary. The process shall focus on how to define and specify the system characteristics of a system. For the purpose of this, it deals with techniques to handle such specification activities (MIL-STD-499B, 1992(Draft); Blanchard et al. 2006; BS ISO/IEC 26702, 2007; BS EN 62347, 2007).

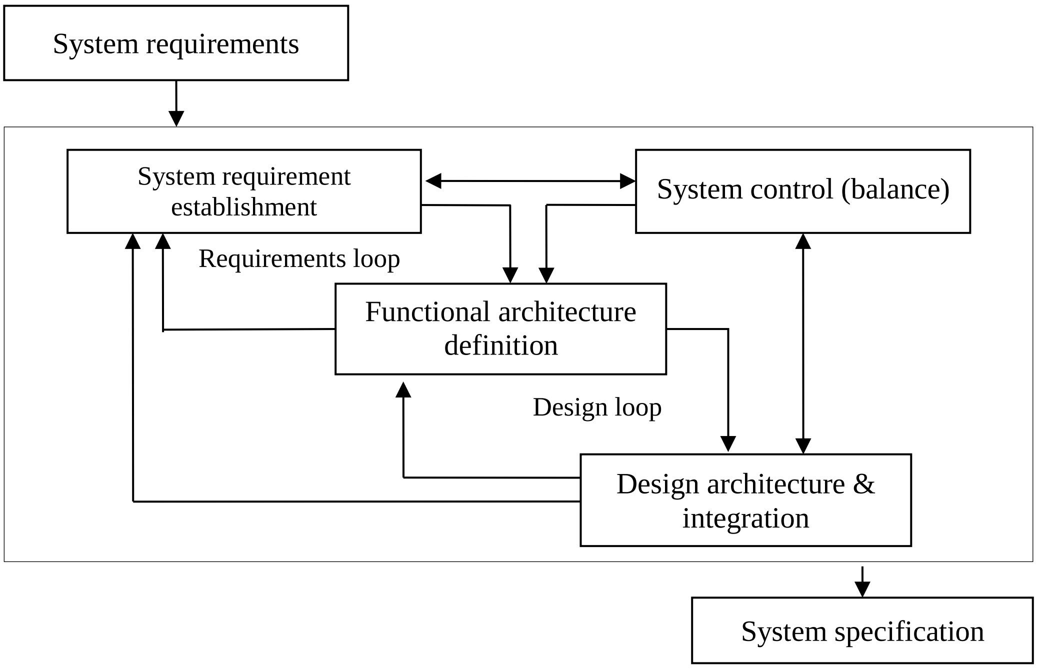

System requirements
System requirement establishment
System control (balance)
Requirements loop
Functional architecture definition
Design loop
Design architecture & integration
System specification

Figure 2 Rolling Stock Specification Process

As shown in Figure 2, the system identification is a preparing activity for the identification of information relevant to a system to be developed like a set of requirements of customer. The information may include the following factors: (1) technical objectives with rationale; (2) system effectiveness factors and acceptance criteria; (3) the critical technical performance measures; and (4) mission. The technical objectives generally become a basis for the specification of the system and trade-off analysis when it difficult to establish requirement due to the insufficient data (MIL-STD-499B (draft), 1992).

The first process activity is to establish functional and performance requirements for the primary functions of a system throughout the analyses of information given from customers. Of course, prior to the establishment of the requirements, the context of influencing conditions and evaluation criteria (i.e. effectiveness factors and technical performance measures) are refined in details. The performance requirements shall be established for all identified functional requirements. They are characterised by the success and acceptance criteria (BS EN 62347, 2007). The functional and performance requirements established are allocated into the lower system level.

The continuing process activity is to allocate the functional and performance requirements established by the previous activity through analyses in order to integrate a functional architecture successively. The functional analysis is performed throughout functional flow diagram (Blanchard et al. 2006) to determine the lower level functions needed. Therefore, it shall be the logical sequence. The functional allocation is to establish performance requirements for each functional requirement. Time requirements are also determined and allocated in the process of functional analysis. The resultant requirements shall be quantitatively defined to use design and acceptance criteria. The established requirements are synthesised into the system configuration functionally and physically.

The third is a process activity for designing the solutions of established functional and performance requirement into a functional architecture, and integrating them into a physical architecture. In this process activity, a complete requirement is established for design; the significant system performance measures are determined; the solutions for the system design, system configuration; and the system characteristics are defined. The functional and physical architecture are transformed into work breakdown structure. The outputs of the process activities are analysed and controlled repeatedly.

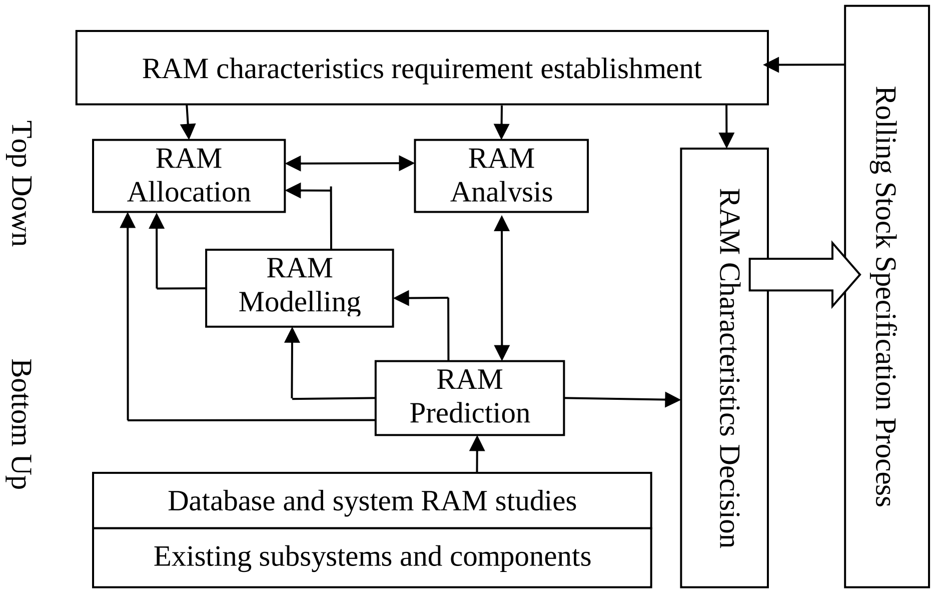

RAM characteristics requirement establishment
Top Down
Bottom Up
RAM Allocation
RAM Analvsis
RAM Modelling
RAM Prediction
Database and system RAM studies
Existing subsystems and components
RAM Characteristics Decision
Rolling Stock Specification Process

Figure 3 A Specification Process for Rolling Stock RAM Characteristics

The final process activity, system analysis and control, is on balancing the results produced in each process activities by means of the measurement of process progression, the evaluation of alternatives, the selection of preferred alternative and the documentation of data and decision making. The system analysis conducts trade-off studies, effectiveness analysis and assessments, and design analyses. Whereas, the control mechanisms execute managements (risk, configuration, data), measurements (performance based progress, technical performance), and technical review.

ROLLING STOCK RAM SPECIFICATION PROCESS

The specification of the system characteristics of a rolling stock aims to realise the functions relevant to the tasks of the system during the system life cycle. Equally, RAM specification process is to determine the performance level of RAM characteristics under system specification process. The specification of RAM requirements determined is commenced after the completion of the functional architecture (BS EN 62347, 2007). RAM specification process is consisted of four process activities.

RAM requirements determination

The RAM requirements of a rolling stock are specified with other system requirements of the system. They include a number of performance measures for RAM characteristics, generally three headings: availability, reliability, and maintenance performance. The selection of the measures is relevant to the nature and type of the system, mission profile, and the application environmental and the criticality of the needed functions of the system (BS EN 50126-1, 1999; BS EN 50126-3, 2006; BS EN 60300-3-4, 2008; Ebling, 2010).

The availability requirements are especially specified in terms of the downtime during the system operation. The reliability requirements are specified for the success of mission without failure. The Maintainability requirements are particularly considered in that it is the great contribution to life cycle cost. The RAM requirements and goals in the specification process are definitely different as shown in Figure 4. The requirements are part of the results of the specification process and the goals are an aspiration of the customers before the specification progresses.

Figure 3 represents the process procedure for determination of RAM requirement. As mentioned above, the availability and reliability goals are determined by the operational objective (e.g. schedule adherence rate or train operation rate of peak period) as mentioned above and then, reliability and maintainability gaols may be trade-off by the availability. The bellows discuss the activities for the RAM requirements.

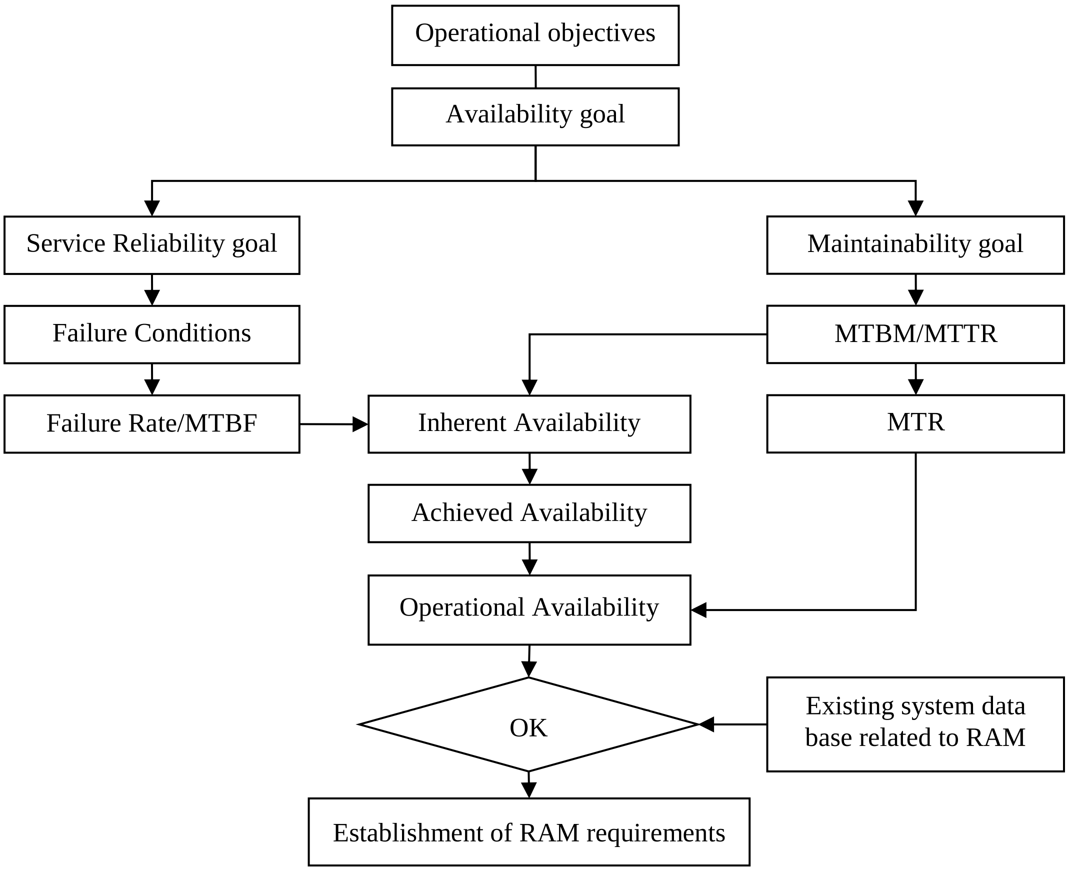


Figure 4 RAM Specification Process Activities for Determination RAM Requirement

Availability performance requirements

For rolling stock, availability is a prime system performance characteristic as described in the procedure above. It is applied at the system level throughout the definition of the down time by Equation 1.1. The downtime is defined because of the high relationship between revenue and service loss of the system, personnel injury due to the system. The downtime of a rolling stock is generally used by the peak periods (e.g. during a day, a weekend, a special holiday (s) etc.) or the maximum delay times of mission profile of the system. The availability is required one or two among defined availabilities: such as steady state availability (or general availability); instantaneous availability; mean availability; and operational availability in order to keep the balance of up time and down time operationally. However, if the failure rate or repair rate of a system are constant, the steady state availability, $A,$ is identical for a first estimate of the availability. The equation 1.1 is the general view that:

$$A = \frac{Uptime}{Uptime + downtime} \tag{1.1}$$

To predict the availability of a system in the specification process, the failure and repair probability of the system applied must be considered because it depends on reliability and maintainability as shown in Equation 1.2~1.4. It is possible for the steady state availability of Equation 1.1 to form three different availabilities according to the definitions of uptime and downtime. The first form is inherent availability (A_i) as illustrated in Equation 1.2. It only considers mean time to failure (*MTBF*) and mean repair time (*MTTR*) and is used as a design parameter and RAM trade-off interpretation.

$$A_i = \frac{MTBF}{MTBF + MTTR} \tag{1.2}$$

The second form is achieved availability, A_a, is defined as described in Equation 1.3. It is applied on the mean maintenance interval (*MTBM*) and mean maintenance time ($\bar{M}$).

$$A_a = \frac{MTBM}{MTBM + \bar{M}} \tag{1.3}$$

The final form is operational availability, A_o, is defined as Equation 1.4. It takes account into mean restore time (*MTR*) included *MTTR*, mean delay time for maintenance (*MDT*), mean delay time for supply (*SDT*). This availability measure is very useful in effectively managing a system in the operating phase, but it is complex.

$$A_o = \frac{MTBM}{MTBM + MTR} \tag{1.4}$$

Reliability performance Requirements

For rolling stock, reliability, or service reliability, is directly applied from availability or railway service performance targets (schedule adherence rate or peak periods). Reliability is the ability of implementation for required function of a system. It represents the probability in terms of planned operating conditions and time interval for constant failure rate (λ) as presented in Equation 1.5:

$$R = e^{-\lambda t} \tag{1.5}$$

Where the reliability, the goal of *R*, is derived from availability or service performance targets as stated above and then the failure rate (λ) is determined by the task interval. In general, reliability measures are defined by alternative measures with the confidence of success in the demonstration: i.e. *MTBF* or mean kilometre between service failure (*MKBSF*) and can be obtained from Equation 1.6 and 1.7:

$$MTBF = \frac{1}{\lambda} \tag{1.6}$$

$$MKBSF = MTBF \ \cdot V \tag{1.7}$$

Where, *V* is the mean speed (*km/h*) for a mission profile.

Prior to defining rolling stock, the failure conditions that are likely to be suffered from the system shall be considered in the early phase. It is defined by the consequence of failure. As mentioned above, failure conditions are derived from the down time of availability equation. BS EN 50126-1 (1999) and 50126-3 (2006) define in details for the functional failure in terms of the failure consequences. In addition, the redundancy is another consideration in the determination of reliability measures. The listed blows are the considerations when determining reliability measures:

- Mission profile;
- Failure conditions (or failure definition);
- Operating and environmental conditions;
- Demonstration methods for system acceptance

Maintainability performance requirements

Maintainability affects the cost of the maintenance and availability. It defines as the ability of a corrective and preventive maintenance action from the failed function of the system. The maintainability therefore is focused on the reduction of a non-operation state due to maintenance. The maintenance time shall be specified by the proper measures as mean repair time or delay time, even maintenance cost. It considers the following lists: operational conditions, maintenance personnel, maintenance policy, maintenance tools, spare part, and demonstration methods. Maintenance goal is derived from availability goal and *MTTR* of maintenance organisation. Equation 1.8 is a formula for the determination of maintainability goal of constant repair rate.

$$M(t) = 1 - e^{-1/MTTR} \tag{1.8}$$

The corrective maintenance is carried out for unexpected failures of a system. It focuses on the operation restoration as soon as possible. Therefore, the maximum interest is the reduction of the maintenance time at the system level. The mean corrective maintenance time (*MTTR* or $\overline{M}_{ct}$) is expressed by the mean repair time (M_{ct_i}) and failure rate (λ_i) of the individual lower system as Equation 1.9:

$$\bar{M}_{ct} = \frac{\sum \lambda_i \cdot M_{ct_i}}{\sum \lambda_i} \tag{1.9}$$

The preventive maintenance is a maintenance method to postpone the wear-out characteristics of a system. It includes the activities to retain a system performance at a system level and functions such as inspection tuning, calibration, time/cycle replacement, and overhaul. Therefore, the maximum interest is the reduction of the maintenance time at the system level. The mean preventive maintenance time ($\overline{M_{pt}}$) is expressed by the mean elapsed time (M_{pt_i}) and frequency of the ith preventive maintenance task in actions per system operating hour as Equation 1.10:

$$\bar{M}_{pt} = \frac{\sum M_{pt_i} \cdot f_{pt_i}}{\sum f_{pt_i}} \tag{1.10}$$

RAM Allocation

The process activity that successively allocates the system level RAM requirements of a system into the lower levels of the system is defined as RAM allocation, which is also a technique for partitioning and mapping the RAM performance characteristics onto the system architectures. The purpose of which is to find the most effective system architecture to achieve the RAMS requirements. The allocation techniques consider the criticality of the system functions as well as operating profile and environmental conditions. The complexity of the system for allocation is determined by the system failure rate or the system life. The suitability of such allocation is recognised by trade-off as Figure 3 (BS EN 60300-2, 2004; BS EN 60706-2, 2006; Ebeling, 2010).

Reliability allocation starts with the completion of reliability block diagram (RBD), which is the extension of functional analysis. MIL-HDBK-388B (1998) presents four reliability allocation methods: (1) Equal Apportionment Technique (EAT); (2) ARINIC Apportionment Technique (ARINIC); (3) Feasibility of objectives Technique; and (4) Minimization of Effort Algorithm. The allocation of system reliability follows the Equation 1.11 and EAT and ARINIC methods are general in the specification process.

$$\prod_{i=1}^{n} R_i(t) \geq R^*(t) \tag{1.11}$$

Equal Apportionment Technique (or exponential case) is used for the absence of definitive information on the systems allocated. The equation is that:

$$\prod_{i=1}^{n} e^{-\lambda t} \geq R^{*}(t) \tag{1.12}$$

$$\sum_{i=1}^{n} \lambda_i = \lambda^{*}$$

ARINIC Apportionment Technique is used under the assumption of constant failure rate (λ^{*}), such that any subsystem failure causes system failure and that the mission time of both system and subsystem are equal. It applies weight factors (W_i) which are considered of failure rate (λ_i) of the each subsystem. Availability is allocated as the same way of reliability allocation.

$$\lambda_i = W_i \lambda^{*} \tag{1.13}$$

$$W_i = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i}$$

Maintainability is mainly conducted for corrective maintenance requirements. It needs the knowledge of system architecture and the RAM performance of the allocated system elements. The maintainability allocation process is generally implemented by two steps as described in Equation 1.14. The first is to separate *MTTR* (M_{ct}) from availability and then allocates the *MTTR* (M_{ct}) into the lower level *MTTR* ($\bar{M}_{ct}$) by the failure rate (λ) and number (N) of the system elements constituted (Blanchard et al. 2006; MIL-HDBK-470A, 1997).

$$M_{ct} = \frac{MTBF(1 - A_i)}{A_i}$$

$$\bar{M}_{ct} = \frac{\sum N \cdot \lambda \cdot M_{ct}}{\sum N \cdot \lambda} \tag{1.14}$$

RAM Prediction

RAM prediction aims to assess the results of RAM allocation, and find out the weak points thereby. It becomes a basis of the determination of RAM specification and it provides design methods. Therefore, RAM prediction is done after RAM specification. Reliability prediction is applied by the methods throughout: (1) the analysis of similar system; (2) an estimate of active system elements; (3) the count of the number of system parts; (4) the analysis of system stress factors; and (5) the analysis of failure mechanism (BS EN 60706-2, 2006; MLL-HDBK-388B, 1998; MIL-HDBK-470B).

Maintainability prediction includes the estimation of maintenance elapsed time factors, maintenance labour hour factors, maintenance frequency factors and maintenance cost factors.

However, generally the mean corrective maintenance ($\bar{M}_{ct}$) is predicted by Equation 1.15 and the mean preventive maintenance ($\bar{M}_{pt}$) are predicted by Equation 1.16.

$$\bar{M}_{ct} = \frac{\sum N \cdot \lambda \cdot M_{ct_i}}{\sum N \cdot \lambda} \tag{1.15}$$

Where, failure rate (λ), quantities of parts (*N*) and M_{ct_i} of a part are applied.

$$\bar{M}_{pt} = \frac{\sum (fpt_i)(N) \cdot M_{pt_i}}{\sum (fpt_i)(N)} \tag{1.16}$$

Where, the task frequency (fpt_i)·(*N*) and the mean task time (M_{pt_i}) are considered.

RAM Trade-Off

RAM trade-off is a decision-making technique for the evaluation of design alternatives possible. The alternatives are specified by the functional allocation process. RAM trade-off may are used for all specification activities by the problem of the RAM evaluation. The RAM trade-off is concerned for reliability and maintainability which is focused on availability and life cycle cost. When an availability requirements are specified, there, if needed, requires trade-off between reliability and maintainability. However, in steady-state, availability in trade-off depends on the ratio of MTTR ($^1/_\mu$)and MTBF ($^1/_\lambda$)or maintenance time ratio (α). In case series subsystems, availability can calculate by Equation 1.17 (BS EN 60300-2, 2004; BS EN 60706-2, 2006; MIL-HDBK-388B, 1998).

$$\alpha = \frac{MTTR}{MTBF} = \frac{\lambda}{\mu}$$

$$A = \frac{1}{(1+\alpha)} = (1+\alpha)^{-1} \tag{1.17}$$

HIGH SPEED TRAIN APPROACH

The high-speed train approach is focusing on the application of proposed RAM process activities (Figure 3 and 4) when specifying the RAM characteristic. The objective of high-speed train is to safely carry passengers like the service quality and journey time of domestic airlines. Therefore, operational service performance target is very high as described in the following below. It is generally derived from the passenger carter, which is performed in many counties.

- Over 95% of all trains shall be arrived within five minutes for published timetable.

It is assumed that the contents of Table 1 are train operating profiles for RAM application:

Table 1 Operational Requirements

NO	Mission profile	New system	Similar system
1	Route length	400 Km	400 Km
2	Journey time	2 hours	2 hours 15 minutes
3	Train operation per each day	3 rounds	2 rounds
4	Service frequency per direction	6 trains	6 trains
5	Non-revenue hours during day	6 hours	6 hours
6	Expected life	25 years	25 years

TARGETS SETTING UP OF RAM CHARACTERISTICS

Determination of RAM Goals and Targets

As shown in the first task of RAM specification process, the assignment of RAM goals are derived from the railway service performance such as schedule adherence and the peak period may be applied. From the service performance target, first of all, availability and reliability goal can be determined from Equation 1.1 and 1.5. The maximum delay time allowed is used by the downtime of the availability and the failure definition of the reliability. The reliability goal is allocated from the schedule adherence rate. And then the failure conditions of a rolling stock are considered prior to determination. Reliability measures are set up by the reliability goal and mission time in terms of Equation 15-17. The maintainability goals are determined by the availability goals and maintenance time possible.

Figure 5 represents the range of reliability goal possible. Reliability targets are established throughout consideration of the data of similar existing system and trade-off technique. As stated in graph, the reliability targets can be applied from over 50000 km (MTBF), but existing system (KTX) which is similar in the operation conditions was applied over 121000 km. Therefore, RAM targets at level of rolling stock can be established as Table 1. The value determined is especially considered the operating trip rounds (similar system: two rounds per day). For RAM targets for main systems is also determined together with the overall RAM targets. It is established by the information of similar system.

Table 1 Determined RAM Targets at Rolling Stock Level

Measures	Availability (%)	Reliability (%)	Maintainability (%)	λ	MTBF (hour)	MTTR (hour)	MKSBF (km)	LIFE (year)
Similar	95.7	99.67	90	0.00165	605	26.7	121000	26
NEW	95.8	99.75	95	0.00125	779	32	159800	25

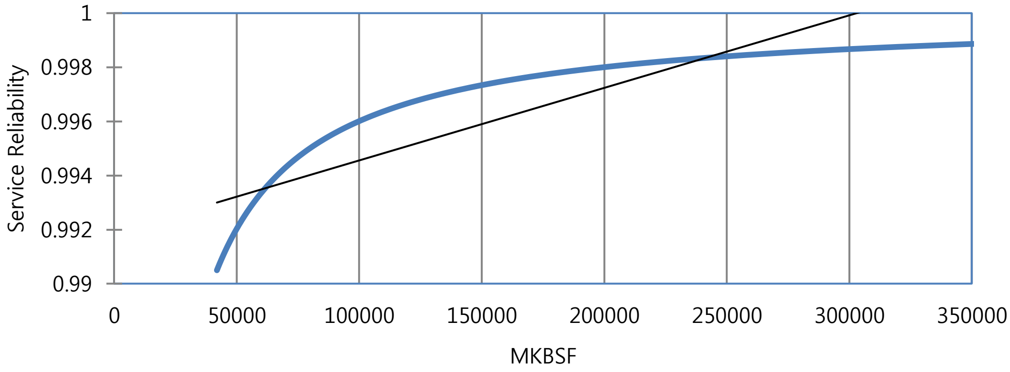


Figure 5 MKBSF for Reliability Probability

Table 2 RAM Targets of Main Systems

Category	λ		MTBF		MTTR	
	Similar	NEW	Similar Hour (year)	NEW Hour (year)	Similar (h)	NEW (h)
Car Body system	1.30E-05	9.92E-06	77016 (26)	100854 (25)	2.2	2.38
Side door system	3.68E-05	2.81E-05	27189 (9.1)	35605 (8.9)	4.0	4.60
High voltage system	1.77E-05	1.36E-04	5634 (1.9)	7378 (1.8)	2.6	2.85
Traction system	2.55E-04	1.95E-04	3915 (1.3)	5127 (1.3)	5.0	5.94
Bogie system	2.39E-04	1.82E-04	4192 (1.4)	5490 (1.4)	3.4	3.83
Braking system	3.52E-05	2.69E-05	28371 (9.5)	37152 (9.3)	2.3	2.50
Cooler/Heating system	4.10E-05	3.13E-05	24384 (8.1)	31931 (8.0)	5.0	5.94
Auxiliary system	2.06E-04	1.57E-04	4863 (1.6)	6368 (1.6)	1.7	1.81
Train control system	6.49E-04	4.96E-04	1540(0.5)	2017 (0.5)	0.5	2.85

RAM Modelling and RAM Target Allocation

Herein, we discuss the methods of modelling and allocating RAM characteristic targets of the propulsion system into the lower level system as illustrated in Figure 7. The propulsion is a main subsystem of a rolling stock that supplies the electrical power of catenary into the traction system. It can be divided by three main functional parts: (1) pantograph equipment that receive the electrical power from catenary and control it (e.g. Pantograph (PAN), Potential transformer (PT), Voltage Circuit breaker (VCB)); (2) Electrical transformer equipment that supply the steady power into the motor block and traction device, (e.g. Roof Equipment (RE), Main Transformer (MT)), and traction system that translate electrical power into movement energy, (e.g. Motor Block (MB), and Traction Motor (TM)). Figure 7 shows their functional block diagram.

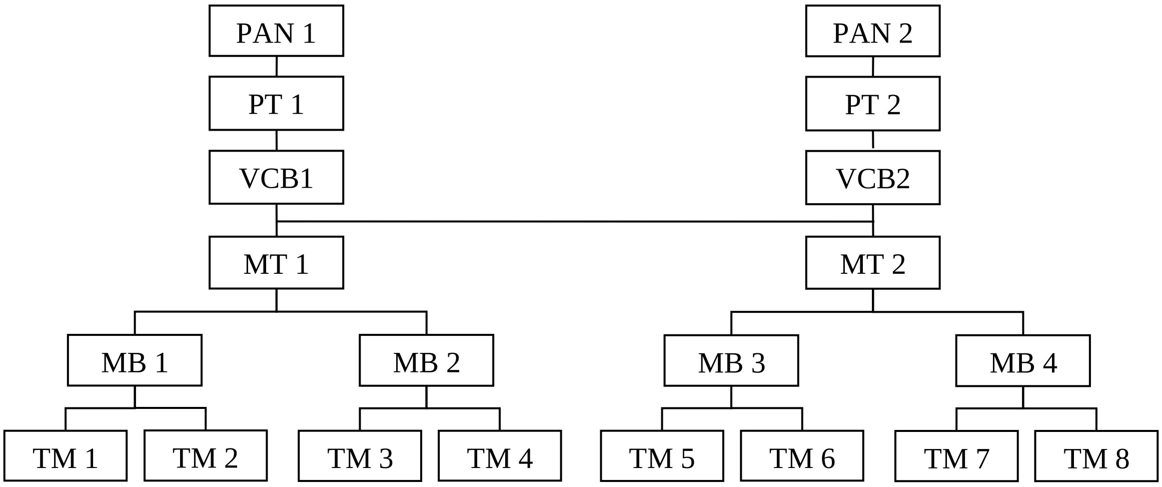


Figure 7 Functional Block Diagram of Propulsion System

This propulsion system is allocated from the rolling stock RAM targets as described in Table 2. It is structured by the combination of the series, parallel and 3 out of 4 structures as shown in Figure 8. For RAM allocation, this system shall be modelled by the series structure. Therefore, this functional structure is modelled by the three groups as mentioned above. The RAM allocation is performed by the ARINIC technique of Equation 1.13 and the weight factor is obtained by the collected data of similar systems. The results are in Table 2.

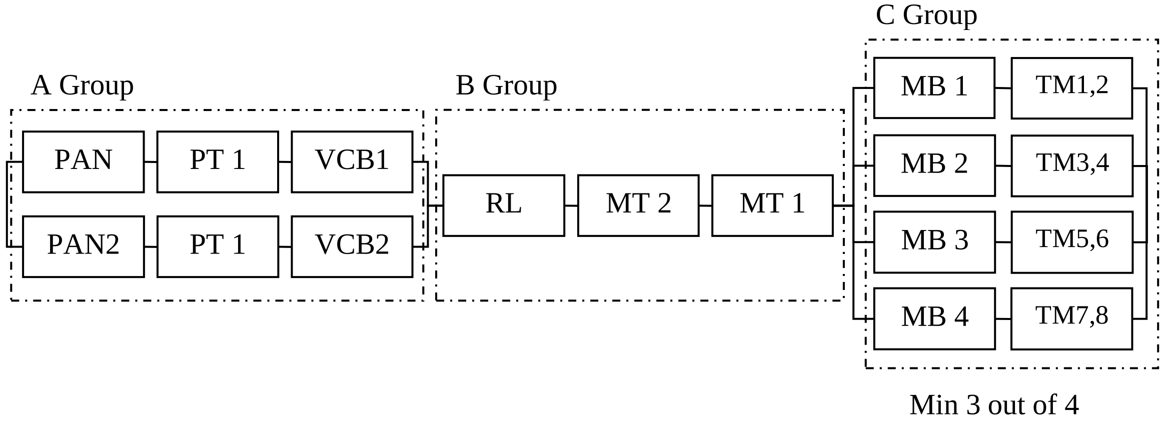


Figure 8 Reliability Block Diagram of Propulsion System

Table 1 RAM Targets of Propulsion System

Population system	λ	MTBF	MKSBF	MTTR
	3.28E-04	3050	610000	4

Table 2 RAM Targets of Subsystem Allocated

Category	λ	MTBF	MKBSF (Km)	MTTR
A Group	0.000328	7114	1422800	1.7
B Group	4.69E-05	21300	4260000	0.6
C Group	0.000328	7114	1422800	1.7

RAM allocation of A Group

A group needs two steps which are simplified for allocation. One allocates after making a modelling of a parallel structure by the use of Equation 2.1 and then making model as two series configuration and allocate within them (Equation 2.2). The equation is like:

$$R = 1 - \left(1 - R_{A_1}\right)\left(1 - R_{A_2}\right) \tag{2.1}$$

$$R_{PAN1} = R_{PT1} = R_{MCB1} = (R_{A1})^{\frac{1}{3}} \tag{2.2}$$

R	$R_{A1=A2}$	$R_{PAN1=PT1=VCB1}$	$R_{PAN2=PT2=VCB2}$
99.93	97.44	99.14	99.14

RAM allocation of B Group

The group B can be simply allocated because of series. Reliability allocated is 0.999906

RAM allocation of C Group

The group C should be allocated by three steps. The first is made up of by four parallel structures and each structure is called C_1 to C_4 and then is allocated by Equation 2.3, 2.4, and 2.5.

$$R_{C1,2,3,4} = 1 - \sqrt[4]{1 - R_C} \tag{2.3}$$

$$R_C = \sum_{x=1}^{4} \binom{4}{x} R_{C_i}^{x} (1 - R_{C_i})^{4-x} \tag{2.4}$$

$$R_{MB1} = R_{TM1} = R_{TM2} = (R_C)^{\frac{1}{3}} \tag{2.5}$$

R	R_{Ci}	R_C	$R_{MBi=TMi}$
99.934	83.997	87.72	94.353

CONCLUSION

Customers require rolling stock with characteristics that are sufficient to their needs and requirements, which are specified throughout the system specification process for effective design characteristics. The specification of RAM characteristics is implemented in the same perspective of system specification process. Therefore, in this paper, we have discussed the engineering activities of specifying RAM characteristics for the improvement of the system effectiveness and life cycle cost of a system. Firstly, we discuss the specification process for defining and specifying system requirements into system architecture throughout the definition of system characteristics. Secondly, the lower structures of the system is integrated and verified into the higher system level configuration for the conformity of the RAM requirements. Finally, RAM performance characteristics are also integrated into the system functions. Examples for the implementation of RAM targets are shown for a practical application of RAM specification.

REFERENCE

Benjamin S. Blanchard and Wolter J. Fabrycky (2006), "**Systems Engineering and analysis**", Person, pp. 17-19, 22-49, 54-91, 369-474

BS ISO/IEC 26702 (2007), "**Systems engineering – Application and management of the systems engineering process**", British standard

BS EN 50126-1 (1999), "**Railway application – the specification and demonstration of RAMS – Part 1: Basic requirements and generic process**", British standard

BS EN 50126-3 (2006), "**Railway application – the specification and demonstration of RAMS – Part 3: Guide to the application of EN 50126-1 for rolling stock RAMS**", British standard

BS EN 60300-1 (2003), "**Dependability management – Part 1: Dependability management systems**", British standard

BS EN 60300-2 (2004), "**Dependability management-Part 2: Guidelines for dependability**

management", British standard

BS EN 60300-4 (2008), "**Dependability management-part 3-4: Application guide-Guide to the specification of dependability requirements**", British standard.

BS EN 60706-2 (2006), "**Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase**", British standard

BS EN 62347 (2007), "**Guidance on system dependability specifications**", British standard

BS EN ISO 9000 (2005), "**Quality management systems – Fundamentals and vocabulary**", British standard

Charles E. Ebling (2010), "**An introduction to reliability and maintainability engineering**". Waveland press, Inc., pp. 171- 192

Marvin Rausand, N. N. Prabhakar Murthy and Trond Osteras, (2008), "**Product Reliability**", Springer, pp. 15-36

MIL-HDBK-388B (1998), "**Electronic Reliability Design Hand Book**", Military standard

MIL-HDBK-470A (1997), "**Design and developing maintainable product and systems**", Military standard

MIL-HDBK-470B, (1989), "**Maintainability program for system and equipment**", Military standard

MIL-STD-499B (1992), "Systems engineering (Draft)" Military standard