BRITISH STANDARD

BS EN
50126:1999

Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

The European Standard EN 50126:1999 has the status of a British Standard

ICS 45.020

National foreword

This British Standard is the English language version of EN 50126:1999.

The UK participation in its preparation was entrusted to Technical Committee GEL/9, Railway electrotechnical applications, which has the responsibility to:

— aid enquirers to understand the text;

— present to the responsible European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;

— monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled "International Standards Correspondence Index", or by using the "Find" facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 70, an inside back cover and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

This British Standard, having been prepared under the direction of the Electrotechnical Sector Committee, was published under the authority of the Standards Committee and comes into effect on 15 December 1999

ISBN 0 580 35694 9

Amendments issued since publication

Amd. No.	Date	Comments

EUROPEAN STANDARD **EN 50126**

NORME EUROPÉENNE

EUROPÄISCHE NORM September 1999

ICS 29.280; 45.020

English version

Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)

Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS)

This European Standard was approved by CENELEC on 1998-10-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national standards bodies of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart, 36 B-1050 Brussels

Ref. No. EN 50126:1999 E

Foreword

This European Standard was prepared by the Technical Committee CENELEC TC 9X, Electrical and electronic applications in railways.

The text of the draft was submitted to the formal vote and was approved by CENELEC as EN 50126 on 1998-10-01.

The following dates were fixed:

–	latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2000-04-01
–	latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2000-04-01

Annexes designated “normative” are part of the body of the standard.
Annexes designated “informative” are given for information only.
In this standard, annexes A to E are informative.

Contents

Figures

Tables

Introduction

This European Standard provides Railway Authorities and the railway support industry, throughout the European Union, with a process which will enable the implementation of a consistent approach to the management of reliability, availability, maintainability and safety, denoted by the acronym RAMS. Processes for the specification and demonstration of RAMS requirements are cornerstones of this standard. This European Standard aims to promote a common understanding and approach to the management of RAMS.

This European Standard can be applied systematically by a railway authority and railway support industry, throughout all phases of the lifecycle of a railway application, to develop railway specific RAMS requirements and to achieve compliance with these requirements. The systems-level approach defined by this European Standard facilitates assessment of the RAMS interactions between elements of complex railway applications.

This European Standard promotes co-operation between a railway authority and railway support industry, within a variety of procurement strategies, in the achievement of an optimal combination of RAMS and cost for railway applications. Adoption of this European Standard will support the principles of the European Single Market and facilitate European railway inter-operability.

The process defined by this European Standard assumes that railway authorities and railway support industry have business-level policies addressing Quality, Performance and Safety. The approach defined in this standard is consistent with the application of quality management requirements contained within the ISO 9000 series of International standards.

1 Scope

1.1 This European Standard:

- defines RAMS in terms of reliability, availability, maintainability and safety and their interaction;
- defines a process, based on the system lifecycle and tasks within it, for managing RAMS;
- enables conflicts between RAMS elements to be controlled and managed effectively;
- defines a systematic process for specifying requirements for RAMS and demonstrating that these requirements are achieved;
- addresses railway specifics;
- does not define RAMS targets, quantities, requirements or solutions for specific railway applications;
- does not specify requirements for ensuring system security;
- does not define rules or processes pertaining to the certification of railway products against the requirements of this standard;
- does not define an approval process by the safety regulatory authority.

1.2 This European Standard is applicable:

- to the specification and demonstration of RAMS for all railway applications and at all levels of such an application, as appropriate, from complete railway routes to major systems within a railway route, and to individual and combined sub-systems and components within these major systems, including those containing software; in particular:
- to new systems;
- to new systems integrated into existing systems in operation prior to the creation of this standard, although it is not generally applicable to other aspects of the existing system;
- to modifications of existing systems in operation prior to the creation of this standard, although it is not generally applicable to other aspects of the existing system.
- at all relevant phases of the lifecycle of an application;
- for use by Railway Authorities and the railway support industry.

NOTE Guidance on the applicability is given in the requirements of this standard.

2 Normative references

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references, the latest edition of the publication referred to applies.

EN ISO 9001	1994	*Quality systems — Model for quality assurance in design, development, production, installation and servicing*
EN ISO 9002	1994	*Quality systems — Model for quality assurance in production, installation and servicing*
EN ISO 9003	1994	*Quality systems — Model for quality assurance in final inspection and test*
EN 50128(*)		*Railway applications — Software for railway control and protection systems*
ENV 50129	1998	*Railway applications — Safety related electronic systems for signalling*
IEC 60050(191)	1990	*International Electrotechnical Vocabulary — Chapter 191: Dependability and quality of service*
IEC 61508	series	*Functional safety of electrical/electronic/programmable electronic safety-related Systems*

(*) In preparation

3 Definitions

For the purposes of this standard, the following definitions apply.

3.1
apportionment
a process whereby the RAMS elements for a system are sub-divided between the various items which comprise the system to provide individual targets

3.2
assessment
the undertaking of an investigation in order to arrive at a judgement, based on evidence, of the suitability of a product

3.3
audit
a systematic and independent examination to determine whether the procedures specific to the requirements of a product comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives

3.4
availability
the ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided

3.5
commissioning
a collective term for the activities undertaken to prepare a system or product prior to demonstrating that it meets its specified requirements

3.6
common cause failure
a failure which is the result of an event(s) which causes a coincidence of failure states of two or more components leading to a system failing to perform its required function

3.7
compliance
a demonstration that a characteristic or property of a product satisfies the stated requirements

3.8
configuration management
a discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control change to those characteristics, record and report change processing and implementation status and verify compliance with specified requirements

3.9
corrective maintenance
the maintenance carried out after fault recognition and intended to put a product into a state in which it can perform a required function

3.10
dependent failure
the failure of a set of events, the probability of which cannot be expressed as the simple product of the unconditional probabilities of the individual events

3.11
down time
the time interval during which a product is in a down state. (IEC 60050(191))

3.12
failure cause
the circumstances during design, manufacture or use which have led to a failure. (IEC 60050(191))

3.13
failure mode
the predicted or observed results of a failure cause on a stated item in relation to the operating conditions at the time of the failure

3.14
failure rate
the limit, if this exists, of the ratio of the conditional probability that the instant of time, T, of a failure of a product falls within a given time interval (t, $t+\Delta t$) and the length of this interval, Δt, when Δt tends towards zero, given that the item is in an up state at the start of the time interval

3.15
fault mode
one of the possible states of a faulty product for a given required function. (IEC 60050(191))

3.16
fault tree analysis
an analysis to determine which fault modes of the product, sub-products or external events, or combinations thereof, may result in a stated fault mode of the product, presented in the form of a fault tree

3.17
hazard
a physical situation with a potential for human injury

3.18
hazard log
the document in which all safety management activities, hazards identified, decisions made and solutions adopted are recorded or referenced. Also known as a ”Safety Log”. (ENV 50129)

3.19
logistic support
the overall resources which are arranged and organized in order to operate and maintain the system at the specified availability level at the required lifecycle cost

3.20
maintainability
the probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources. (IEC 60050(191))

3.21
maintenance
the combination of all technical and administrative actions, including supervision actions, intended to retain a product in, or restore it to, a state in which it can perform a required function. (IEC 60050(191))

3.22
maintenance policy
a description of the inter-relationship between the maintenance echelons, the indenture levels and the levels of maintenance to be applied for the maintenance of an item. (IEC 60050(191))

3.23
mission
an objective description of the fundamental task performed by a system

3.24
mission profile
outline of the expected range and variation in the mission with respect to parameters such as time, loading, speed, distance, stops, tunnels, etc., in the operational phases of the lifecycle

3.25
preventive maintenance
the maintenance carried out at pre-determined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the functioning of an item. (IEC 60050(191))

3.26
railway authority
the body with the overall accountability to a Regulator for operating a railway system

NOTE Railway authority accountabilities for the overall system or its parts and lifecycle activities are sometimes split between one or more bodies or entities. For example:

- the owner(s) of one or more parts of the system assets and their purchasing agents;
- the operator of the system;
- the maintainer(s) of one or more parts of the system;
- etc.

Such splits are based on either statutory instruments or contractual agreements. Such responsibilities should therefore be clearly stated at the earliest stages of a system lifecycle.

3.27
railway support industry
generic term denoting supplier(s) of complete railway systems, their sub-systems or component parts

3.28
RAM programme
a documented set of time scheduled activities, resources and events serving to implement the organizational structure, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given RAM requirements relevant to a given contract or project. (IEC 60050(191))

3.29
RAMS
an acronym meaning a combination of Reliability, Availability, Maintainability and Safety

3.30
reliability
the probability that an item can perform a required function under given conditions for a given time interval (t_1, t_2). (IEC 60050(191))

3.31
reliability growth
a condition characterized by a progressive improvement of a reliability performance measure of an item with time. (IEC 60050(191))

3.32
repair
that part of a corrective maintenance in which manual actions are performed on a item. (IEC 60050(191))

3.33
restoration
that event when an item regains the ability to perform a required function after a fault. (IEC 60050(191))

3.34
risk
the probable rate of occurrence of a hazard causing harm and the degree of severity of the harm

3.35
safety
freedom from unacceptable risk of harm

3.36
safety case
the documented demonstration that the product complies with the specified safety requirements

3.37
safety integrity
the likelihood of a system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time

3.38
safety integrity level (SIL):
one of a number of defined discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety related systems. Safety Integrity Level with the highest figure has the highest level of safety integrity

3.39
safety plan
a documented set of time scheduled activities, resources and events serving to implement the organizational structure, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given safety requirements relevant to a given contract or project

3.40
safety regulatory authority
often a national government body responsible for setting or agreeing the safety requirements for a railway and ensuring that the railway complies with the requirements

3.41
system lifecycle
the activities occurring during a period of time that starts when a system is conceived and end when the system is no longer available for use, is decommissioned and is disposed

3.42
systematic failures
failures due to errors in any safety lifecycle activity, within any phase, which cause it to fail under some particular combination of inputs or under some particular environmental condition

3.43
tolerable risk
the maximum level of risk of a product that is acceptable to the Railway Authority

3.44
validation
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use have been fulfilled

3.45
verification
confirmation by examination and provision of objective evidence that the specified requirements have been fulfilled

NOTE For clarification between verification and validation see Figure 11 and 5.2.9.

4 Railway RAMS

4.1 Introduction

4.1.1 Clause 4 of this standard provides baseline information on the subject of RAMS and RAMS engineering. The purpose of this clause is to provide the reader with sufficient background information to enable the effective application of this standard to railway systems.

4.1.2 Railway RAMS is a major contributor to the Quality of Service provided by a Railway Authority. Railway RAMS is defined by several contributory elements; consequently, this clause of this European Standard is structured as follows:

1) Subclause 4.2 examines the relationship between railway RAMS and quality of service.
2) Subclauses 4.3 to 4.8 examine aspects of railway RAMS, namely:

— the elements of RAMS;
— the factors which influence and means to achieve RAMS;
— risk and safety integrity.

4.1.3 Where possible within this clause, internationally defined terms are used but where new terms are required or where recognized terms have been made specific in the railway context, these are defined in clause 3 of this standard.

4.1.4 Within this European Standard, the sequence ”system, sub-system, component” is used to demonstrate the breakdown of any complete application into its constituent parts. The precise boundary of each term (system, sub-system and component) will depend upon the specific application.

4.1.5 A system can be defined as an assembly of sub-systems and components, connected together in an organized way, to achieve specified functionality. Functionality is assigned to sub-systems and components within a system and the behaviour and state of the system is changed if the sub-system or component functionality changes. A system responds to inputs to produce specified outputs, whilst interacting with an environment.

4.2 Railway RAMS and quality of service

4.1.2 This subclause introduces the link between RAMS and quality of service for an undertaking.

4.2.2 RAMS is a characteristic of a system’s long term operation and is achieved by the application of established engineering concepts, methods, tools and techniques throughout the lifecycle of the system. The RAMS of a system can be characterized as a qualitative and quantitative indicator of the degree that the system, or the sub-systems and components comprising that system, can be relied upon to function as specified and to be both available and safe. System RAMS, in the context of this European Standard, is a combination of reliability, availability, maintainability and safety, RAMS.

4.2.3 The goal of a railway system is to achieve a defined level of rail traffic in a given time, safely. Railway RAMS describes the confidence with which the system can guarantee the achievement of this goal. Railway RAMS has a clear influence on the quality with which the service is delivered to the customer. Quality of Service is influenced by other characteristics concerning functionality and performance, for example frequency of service, regularity of service and fare structure. This relationship is shown in Figure 1.

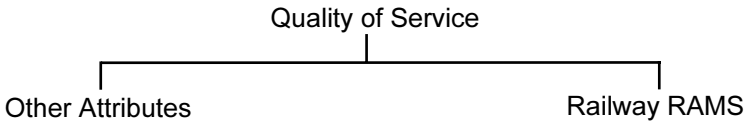


Figure 1 — Quality of Service and Railway RAMS

4.3 Elements of railway RAMS

4.3.1 This subclause introduces the interaction between RAMS elements, reliability, availability, maintainability and safety, in the context of railway systems.

4.3.2 Safety and availability are inter-linked in the sense that a weakness in either or mismanagement of conflicts between safety and availability requirements may prevent achievement of a dependable system. The inter-linking of railway RAMS elements, reliability, availability, maintainability and safety is shown in Figure 2.

4.3.3 Attainment of in-service safety and availability targets can only be achieved by meeting all reliability and maintainability requirements and controlling the ongoing, long-term, maintenance and operational activities and the system environment.

4.3.4 Security, as an element that characterizes the resilience of a railway system to vandalism and unreasonable human behaviour, can be considered as a further component of RAMS. However, consideration of security is outside the scope of this standard.

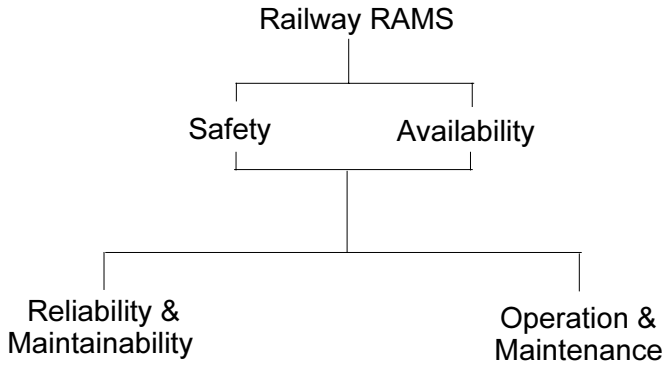


Figure 2 — Inter-relation of Railway RAMS elements

4.3.5 Technical concepts of availability are based on a knowledge of:

a) reliability in terms of:
— all possible system failure modes in the specified application and environment;
— the probability of occurrence of each failure or alternatively, the rate of occurrence of each failure;
— the effect of the failure on the functionality of the system.

b) maintainability in terms of:
— time for the performance of planned maintenance;
— time for detection, identification and location of the faults;
— time for the restoration of the failed system (unplanned maintenance).

c) operation and maintenance in terms of:
— all possible operation modes and required maintenance, over the system lifecycle;
— the human factor issues.

4.3.6 Technical concepts of safety are based on a knowledge of:

a) all possible hazards in the system, under all operation, maintenance and environment modes.

b) the characteristic of each hazard in terms of its severity of consequences.

c) safety/safety related failures in terms of:
— All system failure modes that could lead to a hazard (safety related failure modes). This is a sub-set of all reliability failure modes (a));
— The probability of occurrence of each safety related system failure mode;
— Sequence and/or coincidence of events, failures, operational states, environment conditions, etc., in the application, that may result in an accident. (i.e. a hazard resulting in an accident);
— The probability of occurrence of each of the events, failures, operational states, environment conditions, etc., in the application.

d) maintainability of safety related parts of the system in terms of:
— the ease of performing maintenance on those aspects or parts of the system or its components that are associated with a hazard or with a safety related failure mode;
— probability of errors occurring during maintenance actions on those safety related parts of the system;
— time for restoring the system into a safe state.

e) system operation and maintenance of safety related parts of the system in terms of:
— human factors influence on the effective maintenance of all safety related parts of the system and safe operation of the system;
— Tools, facilities and procedures for effective maintenance of the safety related parts of the system and for safe operation;
— effective controls and measures for dealing with a hazard and mitigating its consequences.

4.3.7 Failures in a system, operating within the bounds of an application and environment, will have some effect on the behaviour of the system. All failures adversely effect the system reliability whereas only some specific failures will have an adverse effect on safety within the particular application. Environment may also influence the functionality of the system and in turn the safety of the railway application. These links are shown in Figure 3.

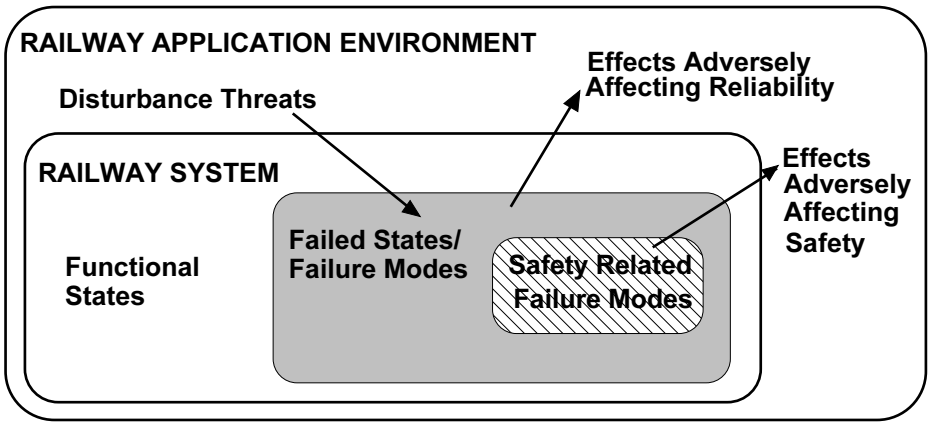


Figure 3 — Effects of Failures Within a System

4.3.8 A dependable railway system can only be realized through consideration of the interactions of RAMS elements within a system and the specification and achievement of the optimum RAMS combination for the system.

4.4 Factors influencing railway RAMS

4.4.1 General

4.4.1.1 This subclause introduces and defines a process to support the identification of factors which influence the RAMS of railway systems, with particular consideration given to the influence of human factors. These factors, and their effects, are an input to the specification of RAMS requirements for systems.

4.4.1.2 The RAMS of a railway system is influenced in three ways, by sources of failure introduced internally within the system at any phase of the system lifecycle (system conditions), by sources of failure imposed on the system during operation (operating conditions) and by sources of failure imposed on the system during maintenance activities (maintenance conditions). These sources of failure can interact. This relationship is shown in Figure 4 and detailed in Figure 5.

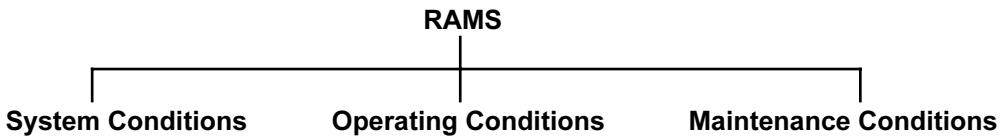


Figure 4 — Influences on RAMS

4.4.1.3 To realize dependable systems, factors which could influence the RAMS of the system need to be identified, their effect assessed and the cause of these effects managed throughout the lifecycle of the system, by the application of appropriate controls, to optimize system performance.

4.4.2 Categories of factors

4.4.2.1 This subclause details a process for the definition of those factors which will affect the successful achievement of a system which complies with specified RAMS requirements.

4.4.2.2 At a high level, the factors which influence system RAMS are generic, applying across all industrial applications. Figure 5 includes some generic factors which influence transport system RAMS. This figure also shows the interaction between these factors. To identify detailed factors which influence the RAMS of railway systems, each generic influencing factor shall be considered in the context of the specific system.

4.4.2.3 An analysis of human factors, with respect to their effect on system RAMS, is inherent within the “systems approach” required by this standard.

4.4.2.4 Human factors can be defined as the impact of human characteristics, expectations and behaviour upon a system. These factors include the anatomical, physiological and psychological aspects of humans. The concepts within human factors are used to enable people to carry out work efficiently and effectively, with due regard for human needs on issues such as health, safety and job satisfaction.

4.4.2.5 Railway applications typically involve a wide range of human groups, from passengers, operational staff and staff responsible for implementing systems to others affected by the railway operation, such as car drivers at level crossings. Each is capable of reacting to situations in different ways. Clearly, the potential impact of humans on the RAMS of a railway system is great. Consequently, the achievement of railway RAMS requires more rigorous control of human factors, throughout the entire system lifecycle, than is required in many other industrial applications.

4.4.2.6 Humans shall be considered as possessing the ability to positively contribute to the RAMS of a railway system. To achieve this aim, the manner in which human factors can influence railway RAMS should be identified and managed throughout the entire lifecycle. This analysis should include the potential impact of human factors on railway RAMS within the design and development phases of the system.

4.4.2.7 Whilst the need to address human factors within the lifecycle is generic, the precise influence of human factors on RAMS is specific to the application under consideration.

4.4.2.8 Generic factors, including those contained in Figure 5, should be reviewed in the context of the railway system under consideration. The Railway Authority shall specify any non-applicable factors in their call for tenders. Each applicable generic factor shall be assessed and detailed influencing factors, specific to the application, systematically derived. Human factors issues, a core aspect within an integrated RAMS management process, shall be addressed within this assessment.

4.4.2.9 The process of deriving detailed influencing factors shall be supported by the use of the two checklists covering railway specific factors (4.4.2.10) and human factors (4.4.2.11), or as an alternative presentation, Figure 5.

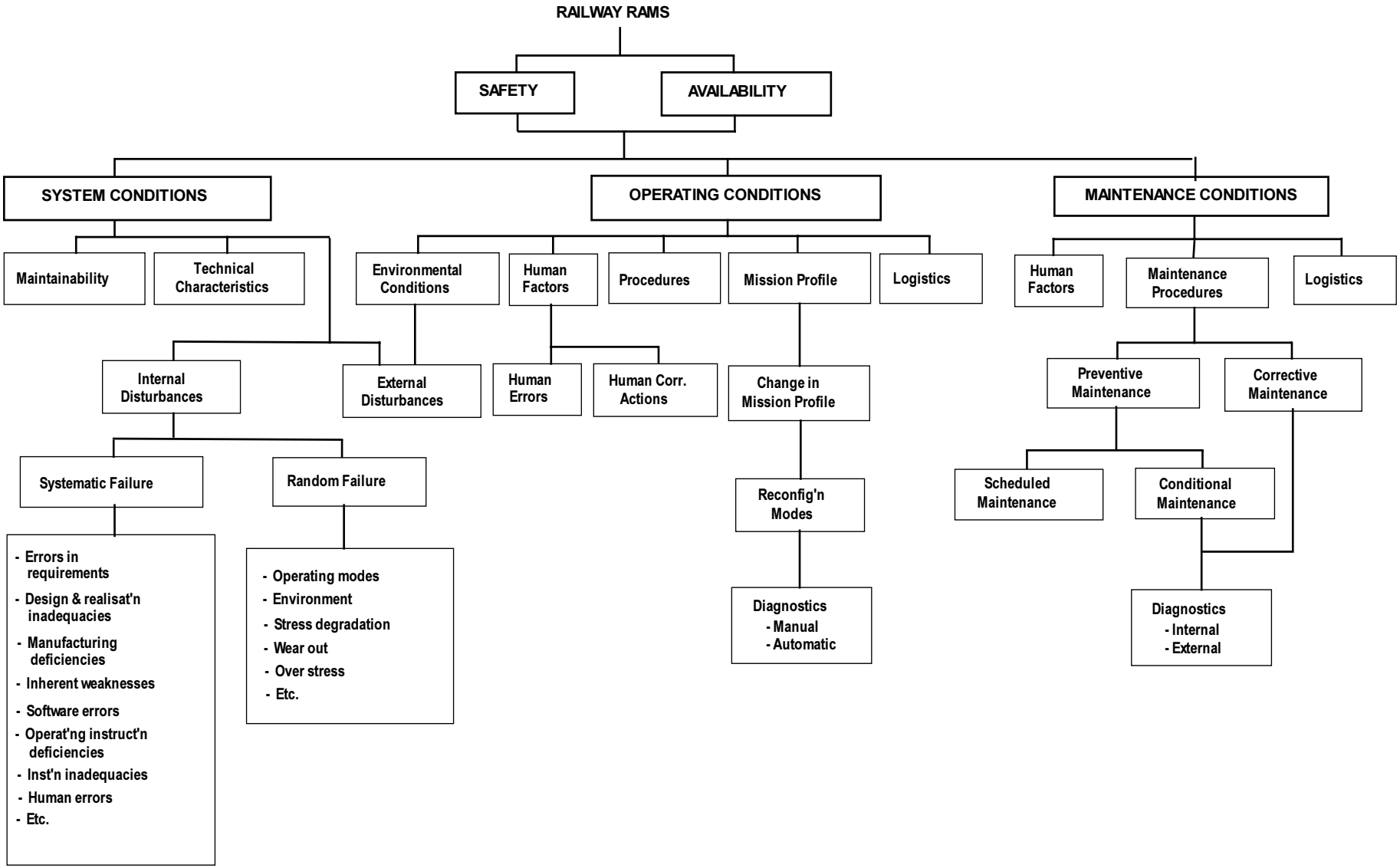


Figure 5 — Factors Influencing Railway RAMS

4.4.2.10 The derivation of detailed railway specific influencing factors should include, but not be limited to, a consideration of each of the following railway specific factors. It should be noted that the following checklist is non-exhaustive and should be adapted to the scope and purpose of the application:

a) system operation:
— the tasks which the system has to perform and the conditions in which the tasks have to be performed;
— the co-existence of passengers, freight, staff and systems within the operating environment;
— system life requirements, including system life expectancy, service intensity and lifecycle cost requirements.

b) environment:
— the physical environment;
— the high level of integration of railway systems within the environment;
— the limited opportunity for testing complete systems in the railway environment.

c) application conditions:
— the constraints imposed by existing infrastructure and systems on the new system;
— the need to maintain rail services during lifecycle tasks.

d) operating conditions:
— trackside-based installation conditions;
— trackside-based maintenance conditions;
— the integration of existing systems and new systems during commissioning and operation.

e) failure categories:
— the effects of failure within a distributed railway system.

4.4.2.11 The derivation of detailed human influencing factors should include, but not be limited to, a consideration of each of the following human factors. It should be noted that the following checklist is non-exhaustive and should be adapted to the scope and purpose of the application.

a) the allocation of system functions between human and machine.

b) the effect on human performance within the system of:
— the human/system interface;
— the environment, including the physical environment and ergonomic requirements;
— human working patterns;
— human competence;
— the design of human tasks;
— human interworking;
— human feedback process;
— railway organizational structure;
— railway culture;
— professional railway vocabulary;
— problems arising from the introduction of new technology.

c) requirements on the system arising from:
— human competence;
— human motivation and aspiration support;
— mitigating the effects of human behavioural changes;
— operational safeguards;
— human reaction time and space.

d) the requirements on the system arising from human information processing capabilities, including:
— human/machine communications;
— density of information transfer;
— rate of information transfer;
— the quality of information;
— human reaction to abnormal situations;
— human training;
— supporting human decision making processes;
— other factors contributing to human strain.

e) the effect on the system of human/system interface factors, including:
— the design and operation of the human/system interface;
— the effect of human error;
— the effect of deliberate human rule violation;
— human involvement and intervention in the system;
— human system monitoring and override;
— human perception of risk;
— human involvement in critical areas of the system;
— human ability to anticipate system problems.

f) human factors in system design and development, including:
— human competency;
— human independence during design;
— human involvement in verification and validation;
— interface between human and automated tools;
— systematic failure prevention processes.

4.4.2.12 A diagrammatic approach to the derivation of detailed factors, such as the use of cause/effect diagrams, is recommended. An example of a much simplified cause/effect diagram is shown in Figure 6.

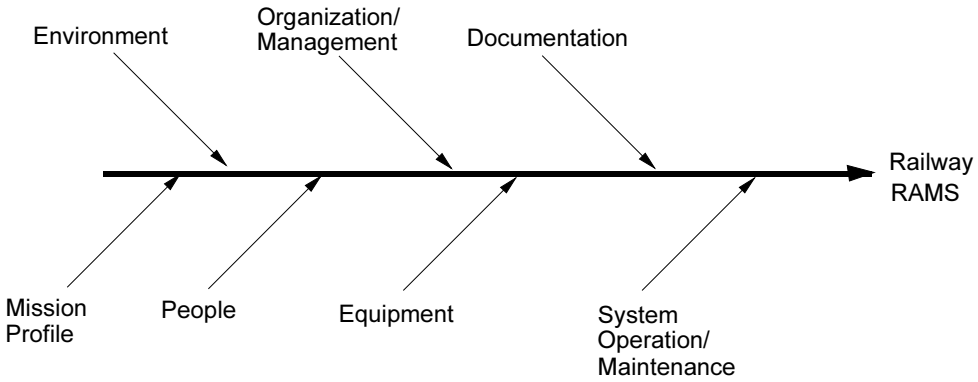


Figure 6 — Example of a Cause/Effect Diagram

4.4.3 Management of factors

The potential effect of each influencing factor on the RAMS of the railway system under consideration shall be evaluated at a level appropriate to the railway system under consideration. This evaluation shall include a consideration of the effect of each factor at each phase of the lifecycle and shall be at a level which is appropriate to the system under consideration. The evaluation shall address the interaction of associated influencing factors. For human factors, the evaluation shall also consider the effect of each factor in relation to each.

4.5 The means to achieve railway RAMS requirements

4.5.1 General

4.5.1.1 The means to achieve railway RAMS requirements relates to controlling the factors which influence RAMS throughout the life of the system. Effective control requires the establishment of mechanisms and procedures to defend against sources of error being introduced during the realization and support of the system. Such defences need to take account of both random and systematic failures.

4.5.1.2 The means used to achieve RAMS requirements are based on the concept of taking precautions to minimize the possibility of an impairment occurring as a result of an error during the lifecycle phases. Precaution is a combination of:

a) prevention: concerned with lowering the probability of the impairment.
b) protection: concerned with lowering the severity of the consequences of the impairment;

4.5.1.3 The strategy to achieve RAMS requirements for the system, including the use of prevention and/or protection means, shall be justified.

4.5.2 RAMS specification

4.5.2.1 The specification of RAMS requirements is a complex process. Annex A of this standard provides an example outline of a RAMS requirements specification, based on the process detailed in this document. Annex B of this standard provides an example outline procedure for the definition of a RAMS programme, based on the requirements of this standard. Both informative annexes are for guidance only and have been populated using rolling stock as an example.

A list of suitable tools for RAMS analysis is also included in annex B. Selection of an appropriate tool will depend on the system under consideration and on factors such as the criticality, novelty, complexity, etc. of the system.

4.5.2.2 Table 1 defines RAM failure categories suitable for use in railway applications.

Table 1 — RAM Failure Categories

Failure Category	Definition
Significant (Immobilizing Failure)	A failure that: prevents train movement or causes a delay to service greater than a specified time and/or generates a cost greater than a specified level
Major (Service Failure)	A failure that: - must be rectified for the system to achieve its specified performance and - does not cause a delay or cost greater than the minimum threshold specified for a significant failure
Minor	A failure that: - does not prevent a system achieving its specified performance and - does not meet criteria for Significant or Major failures

4.5.2.3 Suitable parameters to characterize reliability, availability, maintainability, logistic support and safety requirements of railway systems are shown in annex C (informative). Specific parameters will depend on the system under consideration. All RAMS parameters used should be agreed between the Railway Authority and the Railway Support Industry. Where parameters may be expressed in alternative dimensions, conversion factors should be provided.

4.6 Risk

4.6.1 Risk concept

The concept of risk is the combination of two elements:

— the probability of occurrence of an event or combination of events leading to a hazard, or the frequency of such occurrences;

— the consequence of the hazard.

4.6.2 Risk analysis

4.6.2.1 Risk analysis shall be performed at various phases of the system life cycle by the authority responsible for that phase and shall be documented. The documentation shall contain, as a minimum:

a) analysis methodology;
b) assumptions, limitations and justification of the methodology;
c) hazard identification results;
d) risk estimation results and their confidence levels;
e) results of trade-off studies;
f) data, their sources and confidence levels;
g) references.

4.6.2.2 Table 2 provides, in qualitative terms, typical categories of probability or frequency of occurrence of a hazardous event and a description of each category for a railway system. The categories, their numbers, and their numerical scaling to be applied shall be defined by the Railway Authority, appropriate to the application under consideration.

Table 2 — Frequency of occurrence of hazardous events

Category	Description
Frequent	Likely to occur frequently. The hazard will be continually experienced
Probable	Will occur several times. The hazard can be expected to occur often
Occasional	Likely to occur several times. The hazard can be expected to occur several times
Remote	Likely to occur sometime in the system life cycle. The hazard can reasonably expected to occur
Improbable	Unlikely to occur but possible. It can be assumed that the hazard may exceptionally occur.
Incredible	Extremely unlikely to occur. It can be assumed that the hazard may not occur.

4.6.2.3 Consequence analysis shall be used to estimate the likely impact. Table 3 describes typical hazard severity levels and the consequences associated with each severity level for all railway systems. The number of severity levels and the consequences for each severity level to be applied shall be defined by the Railway Authority, appropriate for the application under consideration.

Table 3 — Hazard Severity Level

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

4.6.3 Risk evaluation and acceptance

4.6.3.1 This subclause deals with the formation of a "frequency - consequence" matrix for evaluation of the results of risk analysis, risk categorization, actions for risk reduction or elimination of intolerable risks, and for risk acceptance.

4.6.3.2 Risk evaluation shall be performed by combining the frequency of occurrence of a hazardous event with the severity of its consequence to establish the level of risk generated by the hazardous event. A "frequency - consequence" matrix is shown in Table 4.

Table 4 — Frequency - Consequence Matrix

Frequency of occurrence of a hazardous event	Risk Levels			
Frequent				
Probable				
Occasional				
Remote				
Improbable				
Incredible				
	Insignificant	Marginal	Critical	Catastrophic
	Severity Levels of Hazard Consequence			

4.6.3.3 Risk acceptance should be based on a generally accepted principle. A number of principles are available that may be utilized. Some examples are as follows: (Also see annex D for more information on these principles):

- As Low As Reasonably Practicable (ALARP principle as practised in UK);
- Globalement Au Moins Aussi Bon (GAMAB principle as practised in France). The complete formulation of this principle is"All new guided transport systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system";
- Minimum Endogenous Mortality (MEM principle as practised in Germany).

Table 5 defines qualitative categories of risk and the actions to be applied against each category. The Railway Authority shall be responsible for defining principle to be adopted and the tolerability level of a risk and the levels that fall into the different risk categories.

Table 5 — Qualitative risk categories

Risk Category	Actions to be applied against each category
Intolerable	Shall be eliminated
Undesirable	Shall only be accepted when risk reduction is impracticable and with the agreement of the Railway Authority or the Safety Regulatory Authority, as appropriate
Tolerable	Acceptable with adequate control and with the agreement of the Railway Authority
Negligible	Acceptable with/without the agreement of the Railway Authority

4.6.3.4 Table 6 shows an example of risk evaluation and risk reduction/controls for risk acceptance.

Table 6 — Typical Example of Risk Evaluation and Acceptance

* Frequency of occurrence of a hazardous event	Risk Levels			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Remote	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Tolerable
Incredible	Negligible	Negligible	Negligible	Negligible
	Insignificant	**Marginal**	**Critical**	**Catastrophic**
	Severity Levels of Hazard Consequence			

* Scaling for the frequency of occurrence of hazardous events will depend on the application under consideration (4.6.2.2)

Risk Evaluation	Risk reduction/control
Intolerable	Shall be eliminated
Undesirable	Shall only be accepted when risk reduction is impracticable and with the agreement of the Railway Authority
Tolerable	Acceptable with adequate control and the agreement of the Railway Authority
Negligible	Acceptable without any agreement

4.7 Safety integrity

4.7.1 When the level of safety for the application has been set and the necessary risk reduction estimated, based on the results of the risk assessment process, the safety integrity requirements, for the systems and components of the application, can be derived. Safety integrity can be viewed as a combination of quantifiable elements (generally associated with hardware, i.e. random failures) and non-quantifiable elements (generally associated with systematic failures in software, specification, documents, processes, etc.). External risk reduction facilities and the system risk reduction facilities should match the necessary risk reduction required for the system to meet its target level of safety.

4.7.2 Confidence in the achievement of the safety integrity of a function within a system may be obtained through the effective application of a combination of specific architecture, methods, tools and techniques. Safety integrity correlates to the probability of failure to achieve required safety functionality. Functions with greater integrity requirements are likely to be more expensive to realize. This standard does not define the correlation between safety integrity and failure probabilities for railway systems, although it should be noted that a generic correlation is defined within draft standard IEC 61508. The definition of this correlation for railway applications is the responsibility of the Railway Authority. However, the management process defined within this standard is generic and suitable for use with any correlation, as agreed by individual authorities or jointly by European Railway Authorities.

4.7.3 Safety functions within systems should be implemented using the architecture, methods, tools and techniques defined in other relevant detailed standards. For example, EN 50128 defines methods, tools and techniques to develop software systems and ENV 50129 defines a process for the acceptance and approval of electronic railway signalling systems.

4.7.4 Safety integrity is basically specified for safety functions. Safety functions should be assigned to safety systems and/or to external risk reduction facilities. This assignment process is iterative, in order to optimize the design and cost of the overall system.

4.7.5 It is the Safety Plan and the RAM Programme which, when implemented effectively, give confidence in the ability of the final system to achieve compliance with RAMS requirements.

4.7.6 The following points concerning product safety integrity shall be noted:

a) the safety functionality required of a system, and its corresponding safety integrity, is influenced by the environment in which the system is used.
b) when a product is developed using methods, tools and techniques appropriate to a specific safety integrity, claims may be made that the product is a safety integrity level ”X” product. This claim means that the product will exhibit specific functionality, within a stated environment, at a certain integrity.
c) Figure 7 shows that the use of commercial "off the shelf" products may differ within different applications. For example Product A is being used to implement different functions within Systems 1 and 2. Consequently, the safety integrity required of a product may differ between applications. Therefore, before applying a product within any system, the limitations and constraints applying to the functionality and the stated environment of the product should be assessed to ensure that they are consistent with the overall requirements of the system.

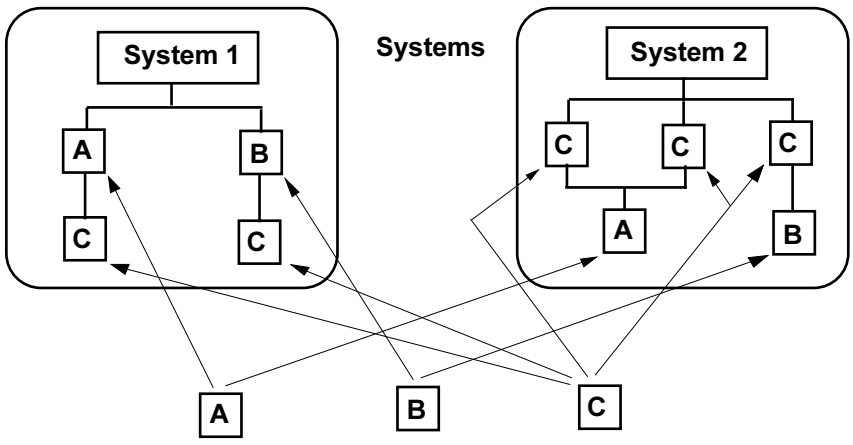


Figure 7 — Certified Products in Safety Systems

NOTE: CENELEC Report R009-001:1997: "Railway Applications - Communication, signalling and processing systems - Hazardous failure rates and safety integrity levels (SIL)" contains further information on safety integrity and safety integrity levels to achieve cross acceptance in Europe. The information and the figures for the railway signalling provided in this report should be handled with much care by experts and, in any case, should not be generalized.

4.7.7 Before applying the concept of SIL, the following requirements should be considered:

a) The adequate level of SIL applicability should be established by safety experts. It is recommended that no more than 4 levels should be used.
b) A SIL shall only be allocated to an "element", namely a stand-alone equipment which performs one or more simple functions and which can be replaced by another one performing the same function(s). Generally, such an "element" is often the lowest level equipment that can be replaced during a first level corrective maintenance operation.
c) Insofar as the environment in which a product will be inserted is of the utmost importance, the extent in terms of SIL to which an off-the-shelf product is certified and what certification means when compared to its safety requirements shall be examined to state whether all the conditions are met for the system under study.
d) A SIL is only addressing an expected level of confidence in the safety for a product. As explained in 4.3 of this standard, safety requirements and availability requirements are inter-related in the context of railway transport. SIL concept does not cover all aspects of a system and therefore considering SIL alone may not be sufficient (e.g. degraded operation modes or fall-back states with different safety requirements, etc.).

4.8 Fail-safe concept

4.8.1 This standard adopts a broad, risk-management approach to safety. This approach is consistent with the fail-safe concept, well established with railway engineers.

4.8.2 From the early days of railways, the inherent fail-safe concept has been used. The concept, dependent upon a set of hypotheses, is based on the use of components with well established failure modes and that a safe condition exists in case of failure of one of its parts. All those components are arranged such that a system, so constructed, cannot allow a more permissive condition than that existing in the absence of a failure.

4.8.3 The validity of the concept is, in general, based on experience but it has limited applicability to the development and use of large, complex systems employing commercial microprocessors. The exponential growth in the number of failure combinations to be considered when using such components means that a deterministic approach is, generally, not practicable. With such complex systems, the probabilistic approach can be used effectively.

4.8.4 The fail-safe approach may be valid for parts of a system and, like other deterministic approaches, it is not precluded by this European Standard. For all approaches, it is necessary to achieve compliance with the specified RAMS requirements for the system.

5 Management of railway RAMS

5.1 General

5.1.1 Clause 5 of this European Standard defines a management process, based on the system lifecycle, which will enable the control of RAMS factors specific to railway applications. The process supports the:

— definition of RAMS requirements;
— assessment and control of threats to RAMS;
— planning and implementation of RAMS tasks;
— achievement of compliance with RAMS requirements;
— on-going monitoring, during the lifecycle, of compliance.

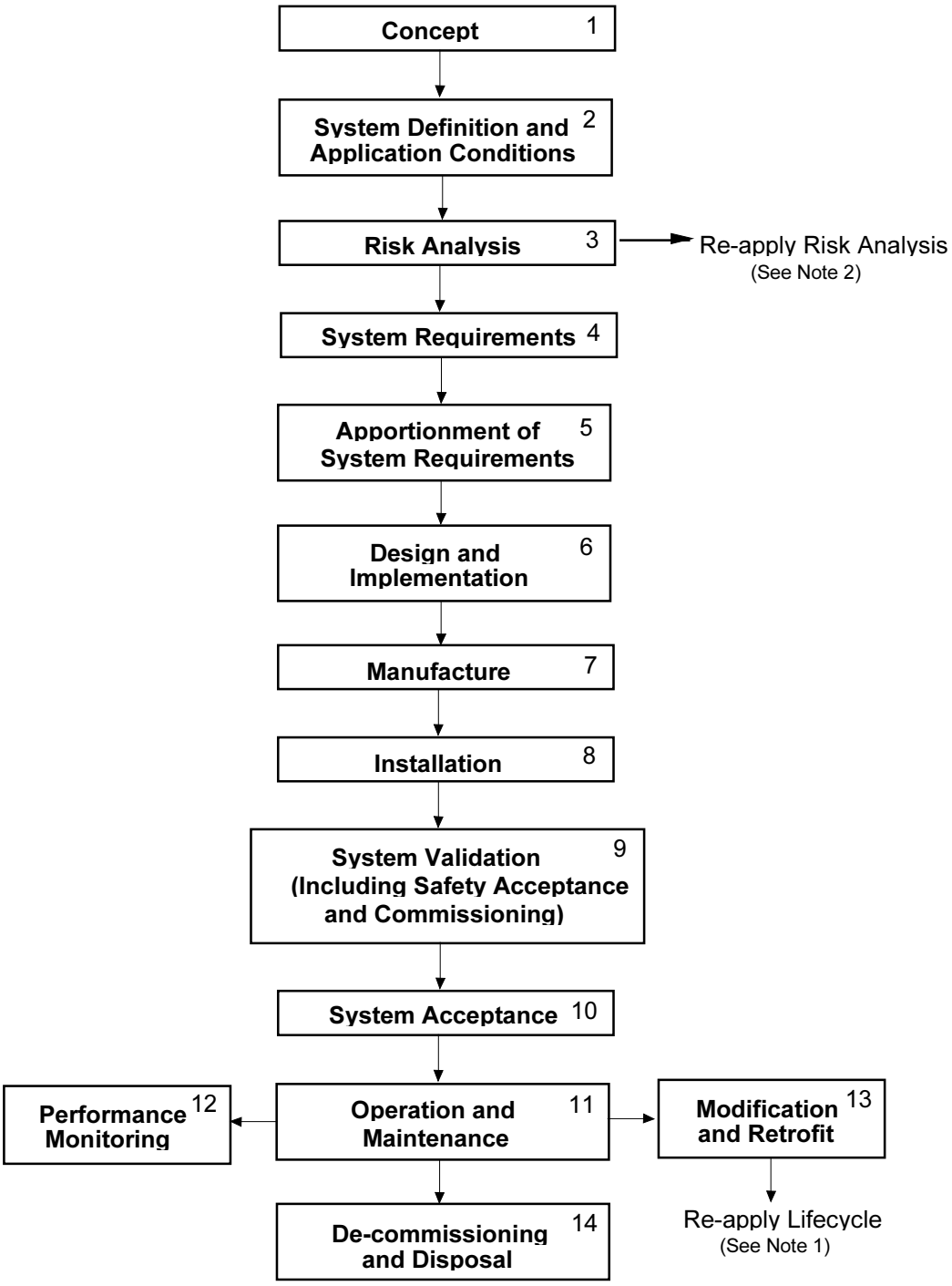
5.1.2 Although railway RAMS is the focus of this European Standard, it is one of many aspects of a total railway system. This clause defines a systematic process for RAMS management such that the process is one component of an integrated management approach which addresses all aspects of the complete railway system.

5.1.3 The tolerable safety risk of a railway system for any Railway Authority is dependent upon the safety criteria set by the national Safety Regulatory Authority, or by the Railway Authority itself in agreement with the Safety Regulatory Authority. The primary responsibility for assessing, controlling and minimizing risk rests with the Railway Authority. In some cases, legislation requires the formal presentation of evidence to demonstrate the adequacy of system safety.

5.2 System lifecycle

5.2.1 The system lifecycle is a sequence of phases, each containing tasks, covering the total life of a system from initial concept through to decommissioning and disposal. The lifecycle provides a structure for planning, managing, controlling and monitoring all aspects of a system, including RAMS, as the system progresses through the phases, in order to deliver the right product at the right price within the agreed time scales. The lifecycle concept is fundamental to the successful implementation of this standard.

5.2.2 Lifecycle, appropriate in the context of railway application, is shown in Figure 8. For each phase of the lifecycle, the main tasks are summarized in Figure 9. This figure shows RAMS tasks as components of general project tasks. The general tasks are outside the scope of this European Standard, but are representative of common industry practice. RAMS tasks contribute to the general project tasks for each phase and requirements for the RAMS tasks are detailed in subsequent clauses of this European Standard.



NOTE 1: The phase at which a modification enters the lifecycle will be dependant upon both the system being modified and the specific modification under consideration

NOTE 2: Risk Analysis may have to be repeated at several stages of the Lifecycle (See item d of 6.3.1)

Figure 8 — System Lifecycle

LIFECYCLE PHASE	PHASE RELATED GENERAL TASKS	PHASE RELATED RAM TASKS	PHASE RELATED SAFETY TASKS
1. CONCEPT	• Establish Scope and Purpose of Railway Project • Define Railway Project Concept • Undertake Financial Analysis & Feasibility Studies • Establish Management	• Review Previously Achieved RAM Performance • Consider RAM Implications of Project	• Review Previously Achieved Safety Performance • Consider Safety Implications of Project • Review Safety Policy & Safety Targets
2. SYSTEM DEFINITION AND APPLICATION CONDITIONS	• Establish System Mission Profile • Prepare System Description • Identify Operation & Maintenance Strategies • Identify Operating Conditions • Identify Maintenance Conditions • Identify Influence of Existing Infrastructure Constraints	• Evaluate Past Experience Data for RAM • Perform Preliminary RAM Analysis • Set RAM Policy • Identify Long Term Op & Mtce Conditions • Identify Influence on RAM of Existing Infrastructure Constraints	• Evaluate Past Experience Data for Safety • Perform Preliminary Hazard Analysis • Establish Safety Plan (Overall) • Define Tolerability of Risk Criteria • Identify Influence on Safety of Existing Infrastructure Constraints
3. RISK ANALYSIS (see Note 6)	• Undertake Project Related Risk Analysis		• Perform System Hazard & Safety Risk Analysis • Set-Up Hazard Log • Perform Risk Assessment
4. SYSTEM REQUIREMENTS	• Undertake Requirements Analysis • Specify System (Overall Requirements) • Specify Environment • Define System Demonstration & Acceptance Criteria (Overall Requirements) • Establish Validation Plan • Establish Management, Quality & Organization Requirements • Implement Change Control Procedure	• Specify System RAM Requirements(Overall) • Define RAM Acceptance Criteria (Overall) • Define System Functional Structure • Establish RAM Programme • Establish RAM Management	• Specify System Safety Requirements (Overall) • Define Safety Acceptance Criteria (Overall) • Define Safety Related Functional Requirements • Establish Safety Management
5. APPORTIONMENT OF SYSTEM REQUIREMENTS	• Apportion System Requirements – Specify Sub-System & Component Requirements – Define Sub-System & Component Acceptance Criteria	• Apportion System RAM Requirements – Specify Sub-System & Component RAM Requirements – Define Sub-System & Component RAM Acceptance Criteria	• Apportion System Safety Targets & Requirements – Specify Sub-System & Component Safety Requirements – Define Sub-System & Component Safety Acceptance Criteria • Update System Safety Plan
6. DESIGN AND IMPLEMENTATION	• Perform Planning • Perform Design and Development • Perform Design Analysis and Testing • Perform Design Verification • Perform Implementation and Validation • Perform Design of Logistic Support Resources	• Implement RAM Programme by Review, Analysis, Testing and Data Assessment, covering: – Reliability & Availability – Maintenance & Maintainability – Optimal Maintenance Policy – Logistic Support • Undertake Programme Control, covering: – RAM Programme Management – Control of Sub-Contractors & Suppliers	Implement Safety Plan by Review, Analysis, Testing and Data Assessment, addressing: • Hazard Log • Hazard Analysis & Risk Assessment • Justify Safety Related Design Decisions • Undertake Programme Control, covering: – Safety Management – Control of Sub-Contractors & Suppliers • Prepare Generic Safety Case • Prepare (if appropriate) Generic Application Safety Case

Figure 9: Project Phase Related Tasks (Sheet 1 of 2)

LIFECYCLE PHASE	PHASE RELATED GENERAL TASKS	PHASE RELATED RAM TASKS	PHASE RELATED SAFETY TASKS
7. MANUFACTURING	• Perform Production Planning • Manufacture • Manufacture and Test Sub-Assembly of Components • Prepare Documentation • Establish Training	• Perform Environmental Stress Screening • Perform RAM Improvement Testing • Commence Failure Reporting and Corrective Action System (FRACAS)	• Implement Safety Plan by: Review, Analysis, Testing & Data Assessment • Use Hazard Log
8. INSTALLATION	• Assemble System • Install System	• Start Maintainer Training • Establish Spare Parts and Tool Provision	• Establish Installation Programme • Implement Installation Programme
9. SYSTEM VALIDATION (INCLUDING SAFETY ACCEPTANCE AND COMMISSIONING)	• Commission • Perform Probationary Period of Operation • Undertake Training	• Perform RAM Demonstration	• Establish Commissioning Programme • Implement Commissioning Programme • Prepare Application Specific Safety Case
10.SYSTEM ACCEPTANCE	• Undertake Acceptance Procedures, based on Acceptance Criteria • Compile Evidence for Acceptance • Entry into Service • Continue Probationary Period of Operation (if appropriate)	• Assess RAM Demonstration	• Assess Application Specific Safety Case
11.OPERATION AND MAINTENANCE	• Long Term System Operation • Perform On Going Maintenance • Undertake On Going Training	• On Going Procurement of Spare Parts & Tools • Perform On Going Reliability Centred Maintenance, Logistic Support	• Undertake On Going Safety Centred Maintenance • Perform On Going Safety Performance Monitoring and Hazard Log Maintenance
12.PERFORMANCE MONITORING	• Collect Operational Performance Statistics • Acquire, Analyse and Evaluate Data	• Collect, Analyse, Evaluate and Use Performance & RAM Statistics	• Collect, Analyse, Evaluate and Use Performance & Safety Statistics
13.MODIFICATION AND RETROFIT	• Implement Change Request Procedures • Implement Modification and Retrofit Procedures	• Consider RAM Implications for Modification & Retrofit	• Consider Safety Implications for Modification & Retrofit
14. DECOMMISSIONING AND DISPOSAL	• Plan Decommissioning and Disposal • Undertake Decommissioning • Undertake Disposal	• No activity for RAM	• Establish Safety Plan • Perform Hazard Analysis & Risk Assessment • Implement Safety Plan

NOTE 1: Change Control or Configuration Management activity applies to all project phases
NOTE 2: Verification and Validation activities apply within most lifecycle phases and are included in the main text
NOTE 3: For RAM, the term “RAM Programme” is in common use & is adopted by this standard. For Safety, the term “Safety Plan” is in common use and is adopted by this standard
NOTE 4: Note that the scope of this standard is limited to RAMS and does not address all systems assurance activities. However, it is necessary to ensure the synchronization between RAMS phases and project related phases, and to agree on the conditions for passing from one phase to another, from RAMS point of view.
NOTE 5: Activities within Phases 9 and 10 may be integrated, depending upon the application under consideration
NOTE 6: Risk analysis may have to be repeated at several stages (see clause 4.6.2 and 6.3.1 d))

Figure 9: Project Phase Related Tasks (Sheet 2 of 2)

5.2.3 This standard acknowledges the balance between the RAMS performance of a system and the costs of development and ownership of the system, known as lifecycle costs. This standard requires a consideration of the lifecycle costs associated with the RAMS aspects of a system. However, it does not dictate solutions to RAMS issues on the basis of cost, as this is the responsibility of the Railway Authority.

5.2.4 Clause 6 and its subclauses define the objectives, requirements, inputs and deliverables for RAMS tasks in a consistent format, and within an overall project context, for each life cycle phase.

5.2.5 The process supports procurement by providing a comprehensive sequence of tasks within lifecycle phases. This provides a basis for the informed contracting of either individual RAMS tasks or a combination of tasks within an integrated management process. Responsibilities for carrying out the tasks will depend on the system under consideration and the contract conditions applicable. Some general guidelines for establishing these responsibilities are given in annex E.

5.2.6 This standard represents the system lifecycle sequentially. This representation shows individual phases and the links between phases. Other lifecycle representations are widespread within industry and include the “V” model.

5.2.7 A “V” representation of the lifecycle contained within this standard is shown in Figure 10. The top-down branch (left side) is generally called development and is a refining process ending with the manufacturing of system components. The bottom-up branch (right side) is related to the assembly, the installation, the receipt and then the operation of the whole system.

5.2.8 The “V” representation assumes that the activities of acceptance are intrinsically linked to the development activities insofar as what is actually designed has to be finally checked in regard to the requirements. So the validation activities for acceptance at various stages of a system are based on the specification of the system and should be planned in the earlier stages, i.e. starting at the corresponding development phases of the lifecycle. Such a link is shown in Figure 11.

5.2.9 This representation is effective in showing verification and validation tasks within the lifecycle. The objective of verification is to demonstrate that, for the specific inputs, the deliverables of each phase meet in all respects the requirements of that phase. The objective of validation is to demonstrate that the system under consideration, at any step of its development and after its installation, meets its requirements in all respects.

5.2.10 In this standard, verification tasks are included within each lifecycle phase. Although this standard is concerned with system assurance in the context of RAMS, verification and validation (V&V) tasks are integral to the overall demonstration of systems assurance. Consequently, RAMS V&V contributes to overall system assurance V&V.

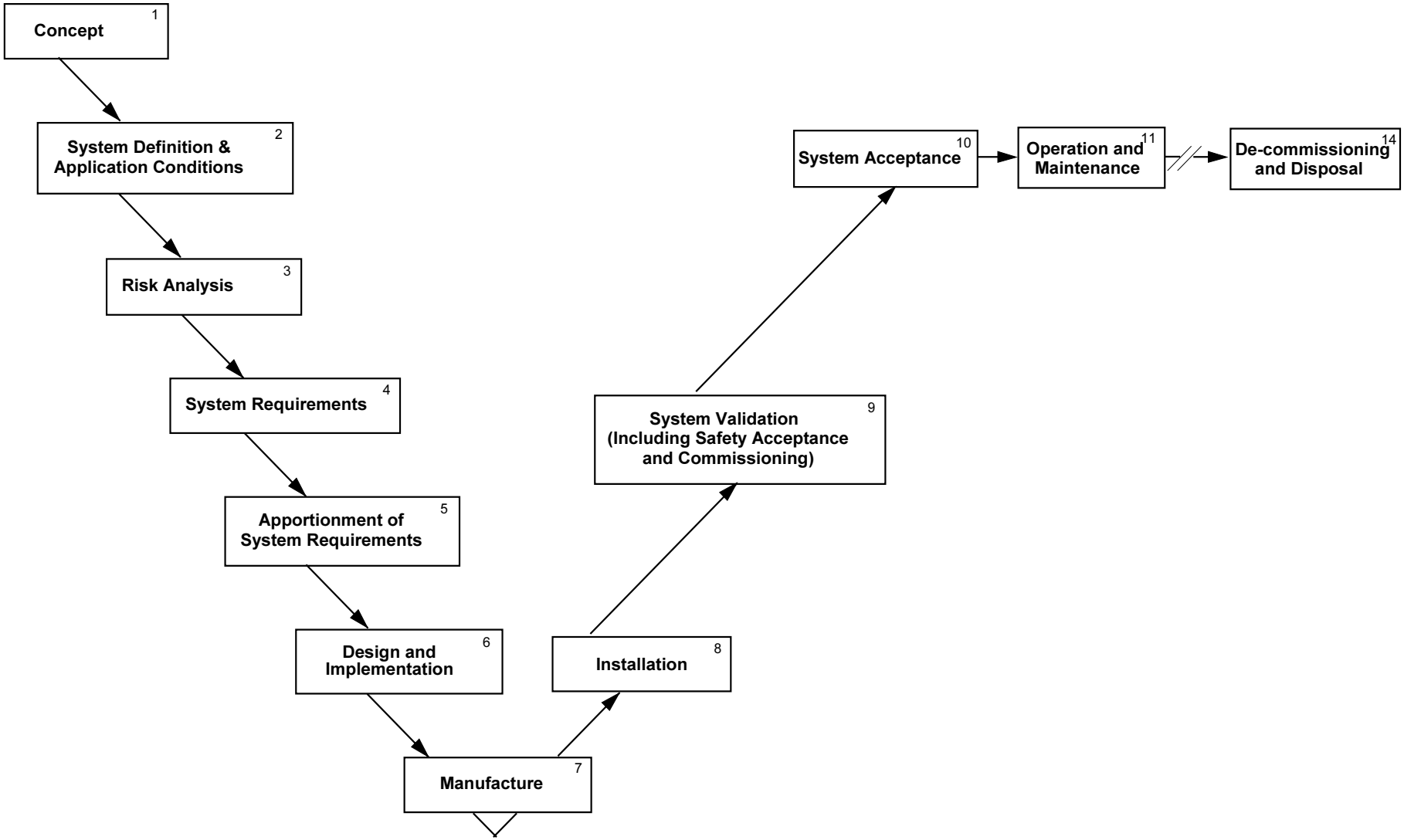
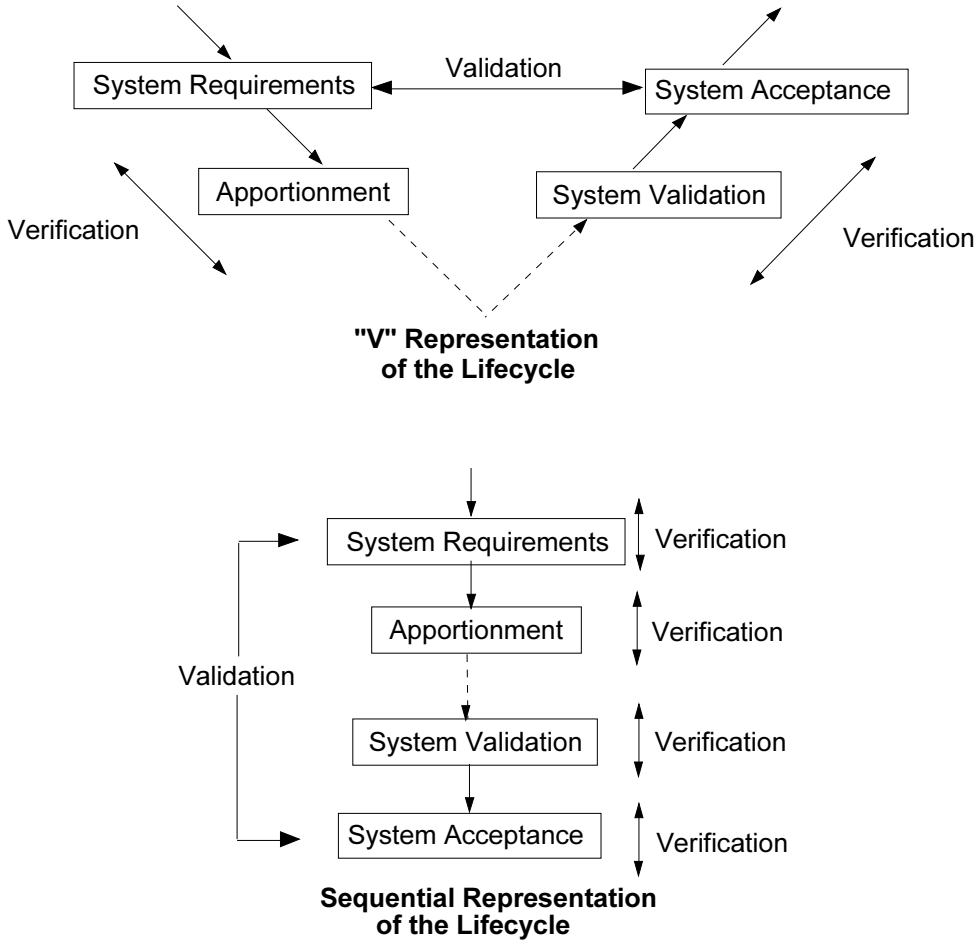


Figure 10 — The “V” Representation



NOTE : Subclause 5.2.9 provides additional information on the role of verification and validation.

Figure 11 — Verification and Validation

5.3 Application of this standard

5.3.1 This subclause gives requirements to provide a flexible and effective application of this standard to railway systems, in terms of size, complexity and cost.

5.3.2 The requirements defined in this standard are generic and are applicable to all types of railway systems. The Railway Authority shall define the application of the requirements of this standard to the system under consideration. This assessment shall be based on the applicability of the requirements to the particular system. Particular care is required during the assessment of the task sequences undertaken in phase 9, System Validation and phase 10, System Acceptance.

5.3.3 In cases of renewal of a system, there is often a "mixed phase" stage where the operation with the existing and the renewed systems is mixed, or that they are operated at the same time. In such cases safety study shall specifically address the possible effects of interaction between the existing and the renewed systems.

5.3.4 The application of this standard shall be adapted to the specific requirements of the system under consideration. The assessment of the application of this standard to the system under consideration shall:

a) specify the lifecycle phases which are required to realize the system under consideration, providing a justification for the lifecycle phases specified and demonstrating that the tasks undertaken within these lifecycle phases comply with the principles of the requirements of this standard.

b) specify the mandatory activities and requirements of each required lifecycle phase, using Figure 9 and the relevant phase related information of clause 6 as a checklist, including:
— the scope of each requirement in relation to the system under consideration;
— the methods, tools and techniques required against each requirement and the scope and depth of their application;
— the verification and validation activities required against each requirement and the scope of their application;
— all supporting documentation.

c) justify any deviation from the activities and requirements of the standard.

d) justify the adequacy of the tasks chosen for the application under consideration.

5.3.5 Within all applications of this standard, the following requirements are mandatory:

a) responsibilities for carrying out all RAMS tasks within each phase of the lifecycle, including the interfaces between associated tasks, shall be defined and agreed for the system under consideration.

b) all personnel with responsibilities within the RAMS management process shall be competent to discharge those responsibilities.

c) the establishment and implementation of the RAM Programme and Safety Plan are essential components in the realization of dependable systems. Whilst the content of these planning documents will be specific to the system under consideration, many RAMS tasks will require similar analysis activities. However, the constraints on these activities may be different. For RAM-focused tasks, cost considerations are likely to be the prime driver, whereas for safety-focused tasks, it is the avoidance of accidents and incidents. Within this context, RAMS requirements can conflict, as the economic consequences pertaining to RAMS may be different, depending upon the requirements of the Railway Authority. Recognition of the need to identify and manage RAMS conflicts shall be included within RAMS planning documents, along with details of all RAMS analysis, as the depth of analysis activities may vary between RAMS tasks.

d) the requirements of this standard shall be implemented within the business processes, supported by a Quality Management System (QMS) compliant with the requirements of EN ISO 9001, EN ISO 9002 or EN ISO 9003 appropriate for the system under consideration.

e) an adequate and effective configuration management system shall be established and implemented, addressing RAMS tasks within all lifecycle phases. The scope of configuration management will depend on the system under consideration, but shall normally include all system documentation and all other system deliverables.

5.3.6 Clause 6 of this standard elaborates the means to ensure achievement of RAMS requirements through minimizing the effects of any impairments and controlling the factors discussed in clause 4, by defining a management process based on the system lifecycle. Methods, tools and techniques appropriate to engineering dependable systems are presented in other standards (see annex B). It is important to note that the choice of methods, tools and techniques, and the depth and scope of their application and that of the documentation, shall be commensurate with the requirements of the system under consideration. These should be agreed between the Railway Authority and the Supplier for the system under consideration. A general overview of the manner in which these different aspects relate to support RAMS engineering and management is shown in Figure 12.

5.3.7 The requirements detailed in this standard are written in order to support an audit process. The Railway Authority and the railway support industry for the system under consideration shall agree and implement an Audit Plan which addresses the application of the requirements of this standard, as adapted to the system.

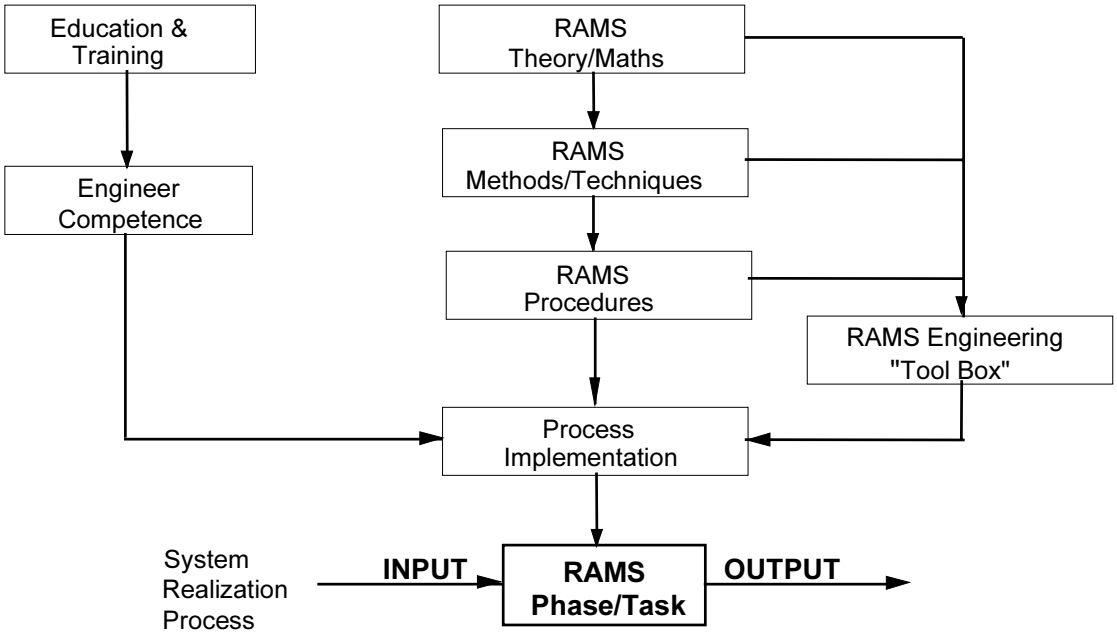


Figure 12 — RAMS Engineering and Management Implemented within a System Realization Process

6 RAMS lifecycle

This clause details objectives, requirements, deliverables and verification and validation activities to be undertaken throughout each lifecycle phase. The scope and application of the requirements shall be assessed and adapted to meet the particular requirements of the system under consideration. For further information on this topic, see 5.3 of this standard.

6.1 Phase 1: Concept

6.1.1 Objectives

The objective of this phase shall be to develop a level of understanding of the system sufficient to enable all subsequent RAMS lifecycle tasks to be satisfactorily performed.

6.1.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirements of the phase, for example the scope and purpose statements for the project.

6.1.3 Requirements

6.1.3.1 Requirement 1 of this phase shall be to acquire, in the context of RAMS performance, an understanding of:

a) the scope, context and purpose of the system.

b) the environment of the system, including:
— physical issues;
— potential system interface issues;
— social issues;
— political issues;
— legislative issues;
— economical issues.

c) the general RAMS implications of the system.

6.1.3.2 Requirement 2 of this phase shall be to review:

a) the RAMS implications of any financial analysis of the system.
b) the RAMS implications of any system feasibility studies.

6.1.3.3 Requirement 3 of this phase shall be to identify sources of hazards which could affect the RAMS performance of the system, including:

— interaction with other systems;
— interaction with humans.

6.1.3.4 Requirement 4 of this phase shall be to obtain information about:

a) previous RAMS requirements and past RAMS performance of similar and/or related systems.
b) identified sources of hazards to RAMS performance.
c) current Railway Authority Safety Policy and Targets.
d) safety legislation.

6.1.3.5 Requirement 5 of this phase shall be to define the scope of the management requirements for subsequent system lifecycle RAMS tasks.

6.1.4 Deliverables

6.1.4.1 The results from this phase shall be documented, along with any assumptions and justifications made during the phase.

6.1.4.2 The deliverables shall include a management structure adequate to implement the RAMS requirements of lifecycle phases 2, 3 & 4

6.1.4.3 The deliverables from this phase are a key input to subsequent lifecycle phases.

6.1.5 Verification

The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to RAMS tasks within this phase.
b) assessment of the adequacy of the system environment statement defined under Requirement 1.
c) assessment of the completeness of the hazard source listing defined under Requirement 3.
d) assessment of the adequacy of the methods, tools and techniques used within the phase.
e) assessment of the competence of all personnel undertaking tasks within the phase.

6.2 Phase 2: System definition and application conditions

6.2.1 Objectives

The objectives of this phase are to:

a) define the mission profile of the system.
b) define the boundary of the system.
c) establish the application conditions influencing the characteristics of the system.
d) define the scope of system hazard analysis.
e) establish the RAMS policy for the system.
f) establish the Safety Plan for the System.

in so far as they affect the potential RAMS performance of the system.

6.2.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirements of the phase, including the deliverables of phase 1.

6.2.3 Requirements

6.2.3.1 Requirement 1 of this phase shall be to define:

a) the system mission profile, including:
— performance requirements;
— RAMS targets;
— long term operating strategy and conditions;
— long term maintenance strategy and conditions;
— system life considerations, including lifecycle costing issues;
— logistic considerations.

b) the system boundary, including:
— interfaces with physical environment;
— interfaces with other technological systems;
— interfaces with humans;
— interfaces with other Railway Authorities.

c) the scope of application conditions influencing the system, including:
— constraints imposed by existing infrastructure;
— system operating conditions;
— system maintenance conditions;
— logistic support considerations;
— review of past experience data for similar systems.

d) the scope of the system hazard analysis, including the identification of:
— hazards inherent within the process to be controlled;
— environmental hazards;
— security hazards;
— the influence of external events;
— the boundaries of the system to be analysed;
— the influence on RAMS of existing infrastructure constraints.

6.2.3.2 Requirement 2 of this phase shall be to perform:

a) preliminary RAM analysis to support targets.
b) preliminary hazard identification to:
— identify sub-systems associated with identified hazards;
— identify types of accident initiating events that need to be considered, including component failure, procedural faults, human error and dependent failure mechanisms;
— define initial risk tolerability criteria.

6.2.3.3 Requirement 3 of this phase shall be to establish the general RAMS policy for the system, including requirements of safety concept and the Railway Authority's' policy for resolving any conflicts arising between "availability" and "safety".

6.2.3.4 Requirement 4 of this phase shall be to establish the Safety Plan for the system. The Safety Plan shall be agreed by the Railway Authority and the railway support industry for the system under consideration and shall be implemented, reviewed and maintained throughout the lifecycle of the system. The Safety Plan should include:

a) the policy and strategy for achieving safety.
b) the scope of the plan.
c) a description of the system.
d) details of roles, responsibilities, competencies and relationships of bodies undertaking tasks within the lifecycle.
e) description of the system lifecycle and safety tasks to be undertaken within the lifecycle along with any dependencies.
f) the safety analysis, engineering and assessment processes to be applied during the lifecycle, including processes for:

— ensuring an appropriate degree of personnel independence in tasks, commensurate with the risk of the system;
— hazard identification and analysis;
— risk assessment and on-going risk management;
— risk tolerability criteria;
— the establishment and on-going review of the adequacy of the safety requirements;
— system design;
— verification and validation;
— safety assessment, to achieve compliance between system requirements and realization;
— safety audit, to achieve compliance of the management process with the safety plan;
— safety assessment to achieve compliance between sub-system and system safety analysis.

g) details of all safety related deliverables from the lifecycle, including:

— documentation;
— hardware;
— software.

h) a process to prepare system Safety Cases.
i) a process for the safety approval of the system.
j) a process for safety approval of system modifications.
k) a process for analysing operation and maintenance performance to ensure realized safety is compliant with requirements.
l) a process for the maintenance of safety-related documentation, including a Hazard Log.
m) interfaces with other related programmes and plans.
n) constraints and assumptions made in the plan.
o) subcontractor management arrangements.
p) requirements for periodic safety audit, safety assessment and safety review, throughout the lifecycle and appropriate to the safety relevance of the system under consideration, including any personnel independence requirements.

6.2.4 Deliverables

6.2.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.2.4.2 The deliverables shall include the RAMS Policy for the system.

6.2.4.3 The deliverables shall include the Safety Plan for the system.

6.2.4.4 The deliverables from this phase form a key input to subsequent lifecycle phases.

6.2.5 Verification

6.2.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase.

b) RAMS aspects of the phase 2 deliverables shall be verified against the phase 1 deliverables, in particular, the RAMS Policy shall be assessed for compliance against the system requirements defined in phase 1.
c) the completeness of the RAM analysis and hazard identification process shall be assessed for completeness.
d) assessment of the adequacy of the Safety Plan, including a review of the adequacy of any data sources included within the Safety Plan.
e) assessment of the adequacy of the methods, tools and techniques used within the phase.
f) assessment of the competence of all personnel undertaking tasks within the phase.

6.2.5.2 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous lifecycle phases.

6.3 Phase 3: Risk analysis

NOTE: Risk analysis may need to be repeated at several stages of the lifecycle (See Item d of 6.3.1 below)

6.3.1 Objectives

The objectives of this phase are to:

a) identify hazards associated with the system.
b) identify the events leading to the hazards.
c) determine the risk associated with the hazards.
d) establish a process for on-going risk management.

6.3.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirements of the phase and in particular, the deliverables produced in phase 2.

6.3.3 Requirements

6.3.3.1 Requirement 1 of this phase shall be to:

a) Systematically identify and prioritize all reasonably foreseeable hazards associated with the system in its application environment, including hazards arising from:
— system normal operation;
— system fault conditions;
— system emergency operation;
— system misuse;
— system interfaces;
— system functionality;
— system operation, maintenance and support issues;
— system disposal considerations;
— human factors;
— occupational health issues;
— mechanical environment;
— electrical environment;
— natural environment to cover such matters as snow, floods, storms, rain, landslides, etc.

b) identify the sequence of events leading to hazards.
c) evaluate the frequency of occurrence of each hazard. (Table 2)
d) evaluate the likely severity of the consequences of each hazard. (Table 3)
e) evaluate the risk to the system for each hazard.

6.3.3.2 Requirement 2 of this phase shall be to determine and classify the acceptability of the risk associated with each identified hazard, having considered the risk in terms of any conflicts with availability and lifecycle cost requirements of the system.

6.3.3.3 Requirement 3 of this phase shall be to establish a Hazard Log as the basis for on-going risk management. The Hazard Log shall be updated, whenever a change to any identified hazard occurs or a new hazard is identified, throughout the lifecycle. Hazard Log shall include details of:

a) the aim and purpose of the Hazard Log;
b) each hazardous event and contributing components;
c) likely consequences and frequencies of the sequence of events associated with each hazard;
d) the risk of each hazard;
e) risk tolerability criteria for the application;
f) the measures taken to reduce risks to a tolerable level, or remove, the risk for each hazardous event;
g) a process to review risk tolerability;
h) a process to review the effectiveness of risk reduction measures;
i) a process for on-going risk and accident reporting;
j) a process for management of the Hazard Log;
k) the limits of any analysis carried out;
l) any assumptions made during the analysis;
m) any confidence limits applying to data used within the analysis;
n) the methods, tool and techniques used;
o) the personnel, and their competencies, involved in the process;

6.3.4 Deliverables

6.3.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.3.4.2 The results of the risk analysis shall be recorded within the Hazard Log.

6.3.4.3 The deliverables from this phase form a key input to subsequent lifecycle phases.

6.3.5 Verification

6.3.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;
b) the phase 3 deliverables shall be verified against the phase 2 deliverables;
c) assessment of the completeness of the risk assessment;
d) assessment of the risk acceptability classification;
e) assessment of the suitability of the hazard log process for the system under consideration;
f) assessment of the adequacy of the methods, tools and techniques used within the phase;
g) assessment of the competence of all personnel undertaking tasks within the phase.

6.3.5.1 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous lifecycle phases.

6.4 Phase 4: System requirements

6.4.1 Objectives

The objectives of this phase are to:

a) specify the overall RAMS requirements for the system.
b) specify the overall demonstration and acceptance criteria for RAMS for the system.

c) establish the RAM Programme for controlling RAM tasks during subsequent lifecycle phases.

6.4.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirements of the phase and in particular, the deliverables of phase 2 and phase 3.

6.4.3 Requirements

6.4.3.1 Requirement 1 of this phase shall be to specify (with reference to 6.2.3.1) the overall RAMS requirements for the total system. The RAMS Requirements, for the system under consideration, shall include:

- definition of the system and boundaries;
- mission profile;
- functional requirements and supporting performance requirements, including safety functional requirements and safety integrity requirements for each safety function;
- logistic support requirements;
- interfaces;
- application environment;
- tolerable risk levels for identified hazards;
- external measures necessary to achieve the requirements;
- system support requirements;
- details of the limits of the analysis;
- details of any assumptions made.

6.4.3.2 Requirement 2 of this phase shall be to specify (with reference to 6.2.3.3) the overall requirements for achieving compliance with RAMS requirements for the system, including:

- acceptance criteria for the overall RAMS requirements;
- demonstration and acceptance process for the overall RAMS requirements facilitated by the system RAMS validation plan, which should include:
- a description of the system;
- the RAMS validation principles to be applied to the system;
- the RAMS tests and analysis to be carried out for the validation including details of the required environment, tools, facilities etc.;
- the validation management structure including requirements for personnel independence;
- details of the validation program (sequence and schedule);
- procedures for dealing with non-compliance.

6.4.3.3 Requirement 3 of this phase shall be to establish the detailed RAM Programme for the remaining lifecycle tasks (with reference to 6.2.3.3). The RAM Programme shall include the tasks which are judged to be the most effective to the attainment of the RAM requirements for the system under consideration. The RAM Programme shall be agreed by the Railway Authority and the railway support industry for the system under consideration and shall be implemented throughout the lifecycle of the system. Within the RAM Programme, consideration should be given to including the following tasks:

a) management, including details of:
- the policy and strategy for achieving RAM requirements;
- the scope of the programme;
- a description of the system;
- the system lifecycle and RAM tasks and processes to be undertaken within the lifecycle, specifically the order of RAM tasks to ensure maximum benefit to system design;

— the roles, responsibilities, competencies and relationships of organizations undertaking tasks within the lifecycle;
— A Failure Reporting Analysis and Corrective Action System (FRACAS) to be applied to the system from phase 7 of the lifecycle (by the Railway Authority and the railway support industry, as appropriate), with records including:
  — technical data on system;
  — reason for maintenance action;
  — type of maintenance action;
  — man-hours & elapsed time for maintenance action;
  — maintenance down time;
  — number and skill level of personnel;
  — spare parts used;
  — cost of consumables;
  — reporting and corrective action.
— the arrangements to ensure co-ordination of individual RAM elements;
— details of all RAM related deliverables from the lifecycle;
— details of RAM acceptance tasks;
— interfaces with other related programmes and plans;
— constraints and assumptions made in the RAM programme;
— subcontractor management arrangements.

b) reliability, including:
— reliability analysis and prediction, including:
  — functional analysis and system failure definition;
  — top down analysis, for example fault tree analysis and block diagram analysis;
  — bottom up analysis, for example Failure Modes Effects Analysis (FMEA);
  — common cause failure or multiple failure analysis;
  — sensitivity analysis and trade-off studies;
  — reliability apportionment;
  — human machine interface analysis;
  — stress analysis;
  — worst case prediction and tolerance analysis.
— reliability planning, including:
  — reliability design review programme;
  — component reliability assurance programme;
  — software quality/reliability assurance programme.
— reliability testing, including:
  — reliability growth testing, based on failure generation;
  — reliability demonstration testing, based on expected failure modes;
  — environmental stress screening;
  — life testing of components;
  — system life testing during early operation.
— reliability data acquisition and assessment;
— data analysis for reliability improvement.

c) maintainability, including:
— maintainability analysis and prediction, including:
  — maintainability analysis and verification;
  — maintenance task analysis;
  — ease-of-maintenance studies and testing;
  — human factors maintainability considerations.
— maintainability planning, including:
  — maintainability design review programme;
  — establishment of the maintenance strategy;

  - review of reliability centred maintenance options;
  - software maintenance programme.
- logistic support evaluation including:
  - definition of maintenance requirements;
  - definition of spares policy and support resource;
  - maintenance personnel and facilities;
  - personnel safety precautions;
  - system support requirements;
  - training programme requirements;
  - system transportation, packaging, handling and storage conditions.
- maintainability data acquisition and assessment;
- data analysis for maintainability improvement.

d) availability, including:
- availability analysis;
- sensitivity analysis and trade-off studies;
- availability demonstration during early operation;
- availability data acquisition and assessment;
- data analysis for availability improvement and prediction.

6.4.3.4 Requirement 4 of this phase shall be to amend the Safety Plan to ensure that all future planned tasks are consistent with the system's emergent RAMS requirements.

6.4.4 Deliverables

6.4.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.4.4.2 The phase shall produce an updated Safety Plan and Acceptance Plan.

6.4.4.3 The deliverables from this phase are an input to subsequent lifecycle phases.

6.4.5 Verification

6.4.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase.
b) system requirements shall be verified against the deliverables produced within phase 2 and phase 3, including lifecycle costings.
c) safety requirements shall be verified against any safety targets and safety policies of the Railway Authority.
d) RAM requirements shall be verified against any RAM targets and RAM policies of the Railway Authority.
e) assessment of the adequacy and completeness of the Acceptance Plan and the Validation Plan.
f) assessment of the adequacy of the RAM Programme, including a review of the adequacy of any data sources used.
g) assessment of the methods, tools and techniques used within the phase.
h) competence assessment of personnel undertaking tasks within the phase.

6.4.5.2 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous lifecycle phases.

6.5 Phase 5: Apportionment of system requirements

6.5.1 Objectives

The objectives of this phase are to:

a) apportion the overall RAMS requirements for the system to designated sub-systems, components and external facilities.
b) define the RAMS acceptance criteria for the designated sub-systems, components and external facilities.

6.5.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirements of the phase and in particular, all deliverables produced in phase 4.

6.5.3 Requirements

6.5.3.1 Requirement 1 of this phase shall be to:

a) allocate functional requirements to designated sub-systems, components and external facilities.
b) allocate safety requirements to designated sub-systems, components and external risk reduction facilities.
c) specify the designated sub-systems, components and external facilities to achieve complete system RAM requirements, including the impact of common cause and multiple failures.
d) review the RAM programme.

6.5.3.2 Requirement 2 of this phase shall be to specify requirements for compliance with sub-system, component and external facilities requirements, including:

— acceptance criteria for sub-system, component and external facilities requirements;
— demonstration and acceptance processes and procedures for sub-system, component and external facilities requirements.

6.5.3.3 Requirement 3 of this phase shall be to review and update the Safety Plan and the Validation Plan to ensure that planned tasks are consistent with the requirements of the system following apportionment. Key areas of concern include requirements for personnel independence and the control of system interfaces where safety functionality may be compromised.

6.5.4 Deliverables

6.5.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.5.4.2 This phase shall produce an updated Safety Plan.

6.5.4.3 The documents resulting from this phase shall include the allocated system requirements to the designated sub-systems, components and external facilities.

6.5.4.4 The deliverables from this phase form a key input to subsequent lifecycle phases.

6.5.5 Verification

6.5.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;

b) verification of system, sub-system, component and external facility requirements against the deliverables produced in phase 4, and including a review of the requirements against the lifecycle cost for the system;
c) the architecture for the total combination of designated sub-systems, components and external facilities shall be verified to ensure it complies with the RAMS requirements for the total system;
d) the RAMS requirements for sub-system, component and external facilities shall be verified to ensure that they are traceable to the RAMS requirements for the system;
e) the RAMS requirements for sub-system, component and external facilities shall be verified to ensure completeness and consistency between functions;
f) the revised Safety plan and Validation plan shall be verified to ensure its continued applicability;
g) assessment of the adequacy of the methods, tools and techniques used within the phase;
h) assessment of the competence of all personnel undertaking tasks within the phase.

6.5.5.2 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous lifecycle phases.

6.6 Phase 6: Design and implementation

6.6.1 Objectives

The objectives of this phase are to:

a) create sub-systems and components conforming to RAMS requirements.
b) demonstrate sub-systems and components conform to RAMS requirements.
c) establish plans for future lifecycle tasks involving RAMS.

6.6.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement, and in particular the deliverables produced in phase 4 and phase 5.

6.6.3 Requirements

6.6.3.1 Requirement 1 of this phase shall be to design the sub-systems and components to meet RAMS requirements.

6.6.3.2 Requirement 2 of this phase shall be to realize the design of the sub-systems and components to meet RAMS requirements.

6.6.3.3 Requirement 3 of this phase shall be to establish plans, in the context of RAMS, for future lifecycle tasks, including:

— installation;
— commissioning;
— operation and maintenance, including definition of operation and maintenance procedures;
— data acquisition and assessment during operation.

6.6.3.4 Requirement 4 of this phase shall be to define, verify and establish a manufacturing process capable of producing RAMS-validated sub-systems and components, giving consideration to the use of:

— environmental stress screening;
— RAM improvement testing;

— inspection and testing for RAMS-related failure modes;
— implementation of requirement 4 of the safety plan (item d of 6.2.3.4).

6.6.3.5 Requirement 5 of this phase shall be to:

a) prepare a Generic Safety Case for the system, justifying that the system, as designed and independent of application, meets safety requirements. The Safety Case requires approval by the Railway Authority, and should include:
— an overview of the system;
— a summary or reference to the safety requirements, including a consideration of the SIL justifications for safety functions;
— a summary of the quality and safety management controls adopted within the lifecycle;
— a summary of safety assessment and safety audit tasks;
— a summary of safety analysis tasks;
— an overview of the safety engineering techniques employed within the system
— verification of the manufacturing process;
— adequacy of compliance with safety requirements, including any SIL requirements of the system;
— a summary of any limitations and constraints applying to the system;
— any special exemption (or specificity) imposed and justified by the contract, to the usual requirements of this Standard.

b) prepare an Application Safety Case, if appropriate at this stage, for the system. The Application Safety Case builds on the Generic Safety Case, justifying that the design of the system and its physical realization, including installation and test phases, for a specific class of application, meet safety requirements. The Application Safety Case requires approval by the Railway Authority, and should include:
— all additional information necessary to justify system safety for the class of application under consideration;
— any limitations or constraints relevant to the application of the system.

6.6.4 Deliverables

6.6.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.6.4.2 A record of all RAMS validation tasks undertaken within the phase shall be maintained.

6.6.4.3 Detailed plans for future lifecycle tasks, in the context of RAMS, shall be produced.

6.6.4.4 Operation and Maintenance Procedures including all the relevant information for providing spare parts, particularly safety related items, shall be produced within this phase.

6.6.4.5 A Generic Safety Case shall be produced within this phase.

6.6.4.6 An Application Safety Case may be produced within this phase.

6.6.4.6 The deliverables from this phase form a key input to subsequent lifecycle phases.

6.6.5 Verification

6.6.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase.
b) verification, by analysis and test, that sub-system and component design complies with the RAMS requirements.

c) verification, by analysis and test, that sub-systems and components realization complies with designs.
d) validation of sub-system and component realization to ensure that the realization complies with RAMS acceptance criteria for sub-system and components, including lifecycle requirements.
e) verification, by analysis and test, that the manufacturing arrangements produce RAMS-validated sub-systems and components.
f) verification that all future lifecycle activity plans are consistent with RAMS requirements for the system, including lifecycle cost requirements.
g) assessment of the adequacy and completeness of the generic safety case and where appropriate, the application safety case.
h) assessment of the adequacy of the methods, tools and techniques used within the phase.
i) assessment of the competence of all personnel undertaking tasks within the phase.
j) ensure the continued applicability of the RAMS validation plan.

6.6.5.2 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous lifecycle phases.

6.7 Phase 7: Manufacturing

6.7.1 Objectives

The objectives of this phase are to:

a) implement a manufacturing process which produces RAMS-validated sub-systems and components;
b) establish RAMS-centred process assurance arrangements;
c) establish sub-system and component RAMS support arrangements.

6.7.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement, and in particular the design deliverables produced in phase 6.

6.7.3 Requirements

6.7.3.1 Requirement 1 of this phase shall be to verify and implement the manufacturing process.

6.7.3.2 Requirement 2 of this phase shall be to establish sub-system and component support arrangements, including:

— preparation, verification and validation of sub-system and component RAMS support documentation;
— preparation, verification and validation of operation and maintenance procedures in the context of RAMS;
— preparation, verification and validation of sub-system and component training material in the context of RAMS.

The above documentation, procedures and training material shall be reviewed in all subsequent phases.

6.7.3.3 Requirement 3 of this phase may, if appropriate, be to:

a) plan manufacturing to meet requirements.
b) implement manufacturing to meet requirements.
c) implement RAMS process assurance to avoid potential RAMS-related failure modes.

6.7.4 Deliverables

6.7.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.7.4.2 A record of all RAMS validation tasks undertaken within the phase shall be maintained.

6.7.4.3 The deliverables from this phase form a key input to subsequent lifecycle phases.

6.7.5 Verification

6.7.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase.
b) verification that RAMS support documentation is correct, adequate and consistent with lifecycle cost requirements and any target RAMS requirements defined for the system.
c) assessment to ensure that the products being produced manufactured comply with system requirements.
d) assessment of the adequacy of the methods, tools and techniques used within the phase.
e) assessment of the competence of all personnel undertaking tasks within the phase.

6.7.5.2 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous lifecycle phases.

6.8 Phase 8: Installation

6.8.1 Objectives

The objective of this phase shall be to:

a) assemble and install the total combination of sub-systems and components required to form the complete system.
b) initiate system support arrangements.

6.8.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement, and in particular the Installation Plan prepared in phase 6, the sub-systems and components manufactured in phase 7 and the RAMS support documentation prepared in phase 7.

6.8.3 Requirements

6.8.3.1 Requirement 1 of this phase shall be to assemble and install the total combination of sub-systems, components and external facilities required to form the complete system, according to the Installation Plan.

6.8.3.2 Requirement 2 of this phase shall be to document the installation process, including:

— review plans in the context of requirement 3 of the design and implementation phase (6.6.3.3);
— installation tasks;
— action taken to resolve failures and incompatibilities.

6.8.3.3 Requirement 3 of this phase shall be to review and update the Safety Plan following completion of installation to ensure that any changes to either system or procedures are recorded and effectively managed in future lifecycle tasks.

6.8.3.4 Requirement 4 of this phase shall be to:

a) start staff training;
b) make support procedures available;
c) establish spare parts provision;
d) establish tool provision.

6.8.4 Deliverables

6.8.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.8.4.2 A record of all RAMS validation tasks undertaken within the phase, including the installation activity, shall be maintained.

6.8.4.3 An updated Safety Plan shall be produced within this phase.

6.8.4.4 The deliverables from this phase form a key input to subsequent lifecycle phases.

6.8.5 Verification

6.8.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;
b) verification that the installation activity was carried out in accordance with the Installation Plan;
c) verification, by analysis and test, that the installed system meets the RAMS requirements;
d) assessment of the safety plan to ensure its continued applicability;
e) assessment of the adequacy and effectiveness of system support arrangements;
f) assessment of the adequacy of the methods, tools and techniques used within the phase;
g) assessment of the competence of all personnel undertaking tasks within the phase.

6.8.5.2 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous lifecycle phases.

6.9 Phase 9: System validation (including safety acceptance and commissioning)

6.9.1 Objectives

6.9.1.1 The objectives of this phase are to:

a) validate that the total combination of sub-systems, components and external risk reduction measures comply with the RAMS requirements for the system.
b) commission the total combination of sub-systems, components and external risk reduction measures.
c) prepare, and if appropriate accept, the Application Specific Safety Case for the system.
d) provide for data acquisition and assessment.

6.9.1.2 It is important to note that the requirements of phase 10, System Acceptance, may be integrated with the requirements of this phase, phase 9, if appropriate to the system under consideration. If this is the case, then the deliverables from this Phase shall demonstrate that the requirements of phase 10 have been adequately fulfilled in the realization of phase 9.

6.9.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement, and in particular the system requirements produced in phase 4, the Verification and Validation Plan produced in phase 4, the Commissioning Plan produced in phase 6 and the training material prepared in phase 7.

6.9.3 Requirements

6.9.3.1 Requirement 1 of this phase shall be to validate the total combination of sub-systems, components and external risk reduction measures according to the Validation Plan and record the validation process, including:

- details of RAMS validation tasks against acceptance criteria, including RAM demonstrations and safety analysis;
- details of process, tools, equipment used for validation tasks against acceptance criteria;
- results of validation tasks for all acceptance criteria;
- any limitations and constraints applying to the system;
- action taken to resolve failures and incompatibilities.

6.9.3.2 Requirement 2 of this phase shall be to:

a) commission the total combination of sub-systems, components and external risk reduction measures according to the Commissioning Plan and record the commissioning process, including:
- commissioning tasks;
- failure reporting and assessment tasks;
- action taken to resolve failures and incompatibilities;
- details of any limitations or constraints on the use of the system.

b) undertake probationary period of operation, if required, to enable the resolution of in-service system problems. Where use is made of a probationary period of operation as part of system acceptance, consideration shall be given to the need for system safety to be demonstrated prior to operation of the system in revenue earning service.

6.9.3.3 Requirement 3 of this phase shall be to prepare an Application Safety Case for the system, if not already prepared in phase 6 (item 2 of6.6.3.5), to justify that the system, as specifically applied within this application, complies with the system safety requirements. The Application Safety Case requires approval by the Railway Authority, and should include:

- an overview of the system;
- a summary or reference to the safety requirements, including a consideration of the SIL justifications for safety functions within the application;
- a summary of the quality and safety management controls adopted within the lifecycle;
- a summary of safety assessment and safety audit tasks;
- a summary of safety analysis tasks;
- an overview of the safety engineering techniques employed within the system;
- adequacy of compliance with safety requirements for the system, including adequacy of compliance with the SIL requirements of the application including its physical realization within the specific application;
- a summary of any limitations and constraints applying to the application.

6.9.3.4 Requirement 4 of this phase shall be to establish and implement a process for the acquisition and assessment of operational data as an input to a system improvement process.

6.9.4 Deliverables

6.9.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.9.4.2 A record of all RAMS validation tasks undertaken within the phase, including the commissioning activity, shall be maintained.

6.9.4.3 An Application Specific Safety Case shall be produced for the system within this phase.

6.9.4.4 A record of all Acceptance Tasks undertaken within this phase shall be maintained.

6.9.4.5 The deliverables from this phase form a key input to subsequent lifecycle phases.

6.9.5 Verification

6.9.5.1 The following process verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase.
b) verification and validation, by analysis and test, that the installed system meets RAMS requirements. It should be noted that for some railway systems, acceptance of the Application Specific Safety Case will be required prior to installation and commissioning activities taking place.
c) verification that the commissioning activity was carried out in accordance with the Commissioning Plan.
d) assessment of the adequacy and effectiveness of the operational data collection system.
e) assessment of the adequacy of the methods, tools and techniques used within the phase.
f) assessment of the competence of all personnel undertaking tasks within the phase.

6.9.5.2 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous lifecycle phases.

6.10 Phase 10: System acceptance

6.10.1 Objectives

The objectives of this phase are to:

a) assess compliance of the total combination of sub-systems, components and external risk reduction measures with the overall RAMS requirements of the complete system.
b) accept the system for entry into service.

6.10.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement, and in particular the system requirements prepared in phase 4, the Verification and Validation Plan and Acceptance Plan prepared in phase 4 and the record of verification and validation tasks prepared in phase 9.

6.10.3 Requirements

6.10.3.1 Requirement 1 of this phase shall be to assess all system verification and validation tasks, specifically the RAM verification and validation and the Application Specific Safety Case, in accordance with the System Acceptance Plan.

6.10.3.2 Requirement 2 of this phase shall be to formally accept the system for entry into service, if appropriate.

6.10.3.3 Requirement 3 of this phase shall be to review and update the Hazard Log to record any residual hazards identified during system validation or acceptance and to ensure that the risks from any such hazards are effectively managed.

6.10.4 Deliverables

6.10.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.10.4.2 A record of all acceptance tasks undertaken within the phase, shall be maintained.

6.10.4.3 An updated Hazard Log shall be produced within this phase.

6.10.4.4 The deliverables from this phase form a key input to subsequent lifecycle phases.

6.10.5 Verification

6.10.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;
b) acceptance, by analysis and test, that the system meets the RAMS requirements, including lifecycle cost requirements;
c) verification that the acceptance activity was carried out in accordance with the Acceptance Plan;
d) assessment of the continued applicability of the revised safety plan;
e) assessment to ensure that any residual hazards are being managed effectively;
f) assessment of the adequacy and completeness of the application specific safety case;
g) assessment of the adequacy of the methods, tools and techniques used within the phase;
h) assessment of the competence of all personnel undertaking tasks within the phase.

6.10.5.2 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous lifecycle phases.

6.11 Phase 11: Operation and maintenance

6.11.1 Objectives

The objective of this phase shall be to operate (within specified limits), maintain and support the total combination of sub-systems, components and external risk reduction measures such that compliance with system RAMS requirements is maintained.

6.11.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement, and in particular the operation and maintenance procedures prepared in phase 6.

6.11.3 Requirements

6.11.3.1 Requirement 1 of this phase shall be to monitor implementation of the system and to implement the operation and maintenance procedures, particularly with regard to system performance and lifecycle cost issues.

6.11.3.2 Requirement 2 of this phase shall be to assure compliance with system RAMS requirements, throughout this phase, by:

a) regular review and update of operation and maintenance procedures;
b) regular review of system training documentation;
c) regular review and update of Hazard Log and Safety Case;
d) effective logistic support, including spare parts, tools, calibration, competent staff, RAMS focused maintenance.
e) maintenance of the failure reporting and corrective action system (FRACAS).

6.11.4 Deliverables

6.11.4.1 A record of all RAMS tasks undertaken within the phase shall be maintained, along with any assumptions and justifications made during the phase.

6.11.4.2 System documentation shall be updated, as appropriate, within this phase.

6.11.4.3 The deliverables from this phase form a key input to subsequent lifecycle phases.

6.11.5 Verification

The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase.
b) verification that changes in support arrangements are consistent with system RAMS requirements and lifecycle cost requirements.
c) assessment of the adequacy of the methods, tools and techniques used within the phase.
d) assessment of the competence of all personnel undertaking tasks within the phase.

6.12 Phase 12: Performance monitoring

6.12.1 Objectives

The objective of this phase shall be to maintain confidence in the RAMS performance of the system.

6.12.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement, particularly system RAMS requirements and system support data.

6.12.3 Requirements

6.12.3.1 Requirement 1 of this phase shall be to establish, implement and regularly review a process for:

— the collection of operational performance and RAMS statistics;
— the acquisition, analysis and evaluation of performance and RAMS data;
— checking that the assumptions made in the safety case remain valid.

6.12.3.2 Requirement 2 of this phase shall be to analyse performance and RAMS data and statistics to influence:

— new operating and maintenance procedures;
— changes in logistic support for the system.

6.12.4 Deliverables

6.12.4.1 A record of all performance monitoring tasks undertaken within the phase shall be maintained, along with any assumptions and justifications made during the phase.

6.12.4.2 System support documentation may be updated within this phase.

6.12.4.3 The deliverables from this phase form a key input to subsequent lifecycle phases.

6.12.5 Verification

The following process verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase.
b) verification that changes in support arrangements are consistent with system RAMS requirements and lifecycle cost requirements.
c) assessment of the adequacy of the methods, tools and techniques used within the phase.
d) assessment of the competence of all personnel undertaking tasks within the phase.

6.13 Phase 13: Modification and retrofit

6.13.1 Objectives

The objective of this phase shall be to control system modification and retrofit tasks to maintain system RAMS requirements.

6.13.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement.

6.13.3 Requirements

6.13.3.1 Requirement 1 of this phase shall be to establish a safety plan.

6.13.3.2 Requirement 2 of this phase shall be to establish, implement and regularly review a process to control system modification and retrofit, in the context of RAMS, including:

— control through the mandatory use of an appropriate lifecycle model for all modification and retrofitting tasks;
— a requirement to establish a procedure for verifying, validating and accepting the RAMS performance of the system following modification and retrofit;
— a requirement to analyse the reasons for the change;
— a requirement to carry out a RAMS impact analysis of the change, including the impact on lifecycle cost requirements;
— a requirement to plan the implementation and subsequent acceptance of the change;
— a requirement to record modification and retrofit tasks;
— a requirement to update all affected system documentation.

6.13.4 Deliverables

6.13.4.1 The key deliverable from this phase is a validated, modified system.

6.13.4.2 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.13.4.3 A record of all verification, validation and acceptance tasks undertaken within the phase, shall be maintained.

6.13.4.4 An updated Hazard Log should be produced within this phase.

6.13.4.5 An updated Application Safety Case shall be produced within this phase.

6.13.4.6 All RAM related documents should be reviewed and updated where necessary.

6.13.4.7 The deliverables from this phase form a key input to subsequent lifecycle phases.

6.13.5 Verification

The following process verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;
b) verify and validate that any changes or modifications to the system are consistent with the RAMS requirements for the system and lifecycle cost requirements;
c) assessment of the adequacy and completeness of any amended system documentation, in particular, any system safety case documents;
d) assessment of the adequacy of the methods, tools and techniques used within the phase;
e) assessment of the competence of all personnel undertaking tasks within the phase.

6.14 Phase 14: Decommissioning and disposal

6.14.1 Objectives

The objective of this phase shall be to control system decommissioning and disposal tasks.

6.14.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement.

6.14.3 Requirements

6.14.3.1 Requirement 1 of this phase shall be to:

a) establish the impact of decommissioning and disposal on any system or external facility associated with the system to be de-commissioned.
b) plan the decommissioning, including the establishment of procedures for:
— the safe closing down of the system and any associated external facility;
— the safe dismantling of the system and any associated external facility;
— the continued assurance of compliance with RAMS requirements of any systems or external facility affected by the decommissioning of the system.

6.14.3.2 Requirement 2 of this phase shall be to provide an analysis of RAMS lifecycle performance for input to future systems, including lifecycle costings.

6.14.4 Deliverables

6.14.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.14.4.2 A record of all de-commissioning and disposal tasks undertaken within the phase, shall be maintained.

6.14.4.3 An updated Hazard Log should be produced within this phase.

6.14.4.4 A Safety Plan should be established to address the de-commissioning and disposal tasks and closed out following completion of the work.

6.14.4.5 A revised Application Safety Case may be produced within this phase.

6.14.4.6 Updated documentation may be produced covering the continued compliance with RAMS requirements of affected associated systems during the decommissioning and disposal tasks.

6.14.5 Verification

The following process verification tasks shall be undertaken within this phase:

a) the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase shall be assessed;
b) assessment of the adequacy of any documentation for systems affected by decommissioning and disposal activities;
c) assessment of the adequacy of the methods, tools and techniques used within the phase;
d) assessment of the competence of all personnel undertaking tasks within the phase.

Annex A (informative)

Outline of RAMS specification - example

A.1 General

In order to facilitate the application of EN 50126, a principal outline of a RAMS specification for railway systems is presented in this annex. This outline example relates to Figure 8 and Figure 9 of the standard and the corresponding descriptions of the lifecycle phases detailed in clause 6, using rolling-stock as an example to provide supporting detail within the outline.

A.2 Outline

The basic structure and contents of a RAMS specification, part of the overall system requirements, may accord with the following outline.

1. Project identification
- 1.1 Identify Project;
- 1.2 Deliverables and deadlines;
- 1.3 Project organization and RAMS Management.

2. General system description
- 2.1 Technical description of system;
- 2.2 Specific application and operation:
  - e.g.: for rolling stock
  - — high speed train operation;
  - — train compositions;
  - — mission profile;
  - — geographical location;
  - — train schedule and tolerances;
  - — operation scenarios;
  - — safety principles;
  - — human factor considerations.
- 2.3 Technical description of sub-systems:
  - e.g.: for rolling stock
  - — energy supply system;
  - — brake system;
  - — propulsion system;
  - — ventilation;
  - — protection system;
  - — control system;
  - — communication system;
  - — heating.

3. Operating and environmental conditions
- 3.1 Identify modes of operation:
  - e.g.: for rolling stock
  - — operating time or distance per day;
  - — stand-by time per day;
  - — off-operating time per day.
- 3.2 Life expectancy:
  - e.g.: for rolling stock
  - — planned total time of system use (years);
  - — average operating time per year.
- 3.3 Identify environmental conditions:
  - e.g.: for rolling stock
  - — standards to follow;
  - — temperature range;

— temperature range of vehicle;
— in operation;
— off-operation;
— humidity range;
— max. height above sea level.

4. Reliability

4.1 Reliability targets:

4.2 Define the reliability targets in order to meet the required performance of the specific application (see item 2.2);

4.3 System Failure Modes and Mean Time Between Failure (MTBF):
e.g.: for rolling stock

Failure Category	System Failure Mode	Effect on Operation	$MTBF_{(.)}$*
Significant	total failure	operation not possible	
Major	critical functional failure	emergency operation 1	
Minor	non-critical functional failure	emergency operation 2	
Negligible	negligible functional failure	normal operation	

* $MTBF_{(.)}$ in hours, years or km.

For further reference see 4.5.2.2 table 1 and annex C, table C.1

4.4 Effect on Operation / Performance :
e.g.: for rolling stock
— Define the technical and operational conditions of what is meant in the application with total failure, emergency operation 1, emergency operation 2 and failures with no effect on operation;

Failure Category	Effect on Operation*	Performance			Remarks
		Power (%)	Speed (%)	(.)	
Significant	operation not possible	0	0		
Major	emergency operation 1				
Minor	emergency operation 2				
Negligible	normal operation	100	100		reduced inf. display

* Define the technical and operational conditions in the application with respect to:
- total failure;
- emergency operation 1;
- emergency operation 2;
- failures with no effect on operation

5. Maintenance and repair

5.1 Preventive Maintenance:

Description of the maintenance policy and the types of Revision R0-R3 encountered.

e.g.: rolling-stock

Type of Revision	MTBM (.)	MTTM (.)
R0		
R1		
R2		
R3		

MTBM: Mean Time Between Maintenance (hours. years or km)
MTTM: Mean Time To Maintain (mean duration of revision in hours or days)

For further reference see annex C, Table C.2 and Table C.4

5.2 Repair:

Description of the repair policy and the necessary logistic support.

- Specify the MTTR (Mean Time To Restore) of the system (in hours or days);
- Define the time elements which are comprised in the MTTR:
  - call / travel time;
  - access time;
  - time for spare parts provision (Logistics);
  - repair / replacement time;
  - test / start-up time;
  - data acquisition time;
  - waiting time.
- Specify the repair / replacement time and conditions of each repairable unit (maximum or mean repair / replacement times);
- Specify minimum spare parts provision and logistics support conditions;

Example:

Repairable Unit	Mean Repair Replacement Time	Site of Repair (field, shop)	Necessary Number of Repair Men

6. Safety

6.1 Safety Targets:

- Describe the safety targets and policy of the application (see item 2.2).

6.2 Hazardous Conditions:

- Identify and list the Hazards to be considered in the application;
- Specify the hazard probability levels (see 4.6.2.2, Table 2).

6.3 Safety related Functions and Failures:

- Identify and list the safety related functions, e.g.: Braking, or units, e.g.: Brake;
- Specify for each safety related function the safety related failures in the application. (see also 4.36 and 4.3.7):

e.g.: rolling-stock

Safety related function / unit	Specification of safety related failure	MTBSF* (years or km)
Braking		
Coach door		

* see annex C, Table C.5

- Safety Hazard Severity Levels:;
- Define the applicable safety hazard severity levels (see4.6.2.3, table 3);
- Risk Classification;
- Define the tolerability of risks (see 4.6.3.2 and 4.6.3.3).

7. Availability

The System Availability A may be specified in parts attributed to:

- planned Non-Availability (Maintenance): $1 - A_M$
- unplanned Non-Availability (Repair): $1 - A_R$
- $A = 1 - [(1 - A_M) + (1 - A_R)]$
- $A = MUT/(MUT + MDT)$; $0 \leq A \leq 1$
- where,
- MUT = Mean Up Time; substitute as appropriate MTBF, MTBSF, etc.
- MDT = Mean Down Time; substitute as appropriate MTTM, MTTR, etc.
- MUT and MDT to be defined for the specific Availability $A_{(.)}$
- e.g. for the Availability A_S of the “safe system”, (MUT ≡ MTBSF).
- The resulting down time $d(T)$ of the mission time T (e.g., 1 year) is:
- $d(T) = (1 - A) * T$

7.1 Availability Specification:

- specify the system availability A in conjunction with the maintenance and repair requirements (item 5);
- the Maintenance and Repair Policy, on which a certain availability A is based, shall be stated.

8. Demonstration of RAMS-performance

Define the Demonstration of RAMS-Performance in line with phase 9: System validation and phase 10: System acceptance.

Demonstration of RAMS-Performance is facilitated by compiling evidence, such as:

- RAMS Management and Organization;
- Availability of RAMS Resources;
- RAMS Requirements Specification;
- RAMS Plans and Programs;
- RAMS related review reports;
- RAMS analysis reports;
- RAMS Testing Records (components);
- Failure Data Acquisition (Statistics);
- Application Specific Safety Case;
- System Validation and Acceptance;
- RAMS Performance Monitoring during early operating phase;
- Life Cycle Cost Evaluation.

9. RAMS programme

A RAM programme and Safety plan shall be devised by the supplier that is judged to be the most effective for the attainment of the RAMS requirements for the project.

Example of a basic RAMS programme is presented in annex B.

Annex B (informative)

RAMS programme

B.1 This annex gives an example of an outline procedure for a basic RAM programme/safety plan and shows an example of a basic RAMS programme (RAM programme/safety plan). It also lists some methods and tools for RAMS management and analysis.

B.2 The supplier should establish a RAMS Programme which will effectively facilitate meeting the RAMS requirements of the application under consideration. The RAMS Programs of similar projects or system requirements of a supplier may yield a “standard RAMS program” which establishes the ”RAMS-Baseline” of a company.

B.3 Procedure:

An outline example procedure for a basic RAMS Programme is given below.

1. Define the appropriate life cycle which is in line with the company’s business process.
   Result: The company’s life cycle or project phases are established.
2. Assign to each project phase the phase related RAM and safety tasks which are necessary to confidently meet the project and system specific requirements.
   Result: All necessary RAMS tasks in the life cycle are identified.
3. Define the responsibilities in the company to carry out each RAMS task.
   Result: The responsible staff and necessary RAMS resources are identified.
4. The necessary instructions, tools and reference documents for each RAMS task are defined.
   Result: Documented RAMS Management.
5. The RAMS activities are implemented in the processes of the company.
   Result: Process integrated RAMS Management (RAMS-Baseline).

B.4 Basic RAMS programme example:

An outline for a basic RAMS Programme is given in table B.1. The outline consists of an example of a set of tasks which could be applied to a particular project.

Table B.1 — Example of a Basic RAMS Programme Outline

Project-Phase	RAMS Tasks	Responsi-bility	Reference-Document
Pre-Acquisition	Evaluate RAMS targets of specific application		
Feasibility Study	– Evaluate RAMS requirements – Evaluate past data and experience of RAMS – Identify influence on Safety imposed by specific application – Consult customer on RAMS (if necessary)		
Invitation for Tenders	– Perform preliminary RAMS analysis (Worst case) – Apportion system RAMS requirements (Sub- systems/ equipment, other relevant systems, etc.) – Perform system hazard & safety risk analysis – Perform RAM related risk analysis – Prepare for future RAMS data assessment – Clause to clause comments concerning RAMS		
Contract Negotiations	– Review/update preliminary RAMS analysis and RAMS apportionment		
Order Processing:- Definition of system requirements	– Establish project specific RAMS management – Specify system RAMS requirements (overall) – Establish RAMS programme (Standard RAMS programme sufficient?) – Assign RAMS requirements to sub-contractors, suppliers – Define RAMS acceptance criteria (overall)		
Order Processing: Design and Implementation	– Reliability analysis (FMEA) – Safety analysis (FMECA), if applicable – Maintenance/repair analysis; define maintenance/repair policy – Availability analysis based on the maintenance/repair policy – RAMS reviews – Life Cycle Cost estimation – RAMS demonstration, evidence compilation – Design/manufacturing FMEA – Reliability and maintainability testing, if applicable		
Procurement	– Provide RAMS specification for sub-contractors/suppliers		
Manufacturing / Testing	– RAMS related quality assurance/process assurance		
Commissioning / Acceptance	– Perform RAM demonstration – Prepare application specific Safety Case – Initiate RAMS data assessment – RAM testing during early operation, data screening and evaluation		
Operation / Maintenance	– Provisional operation and maintenance (Maintenance/repair policy) – Operation and maintenance personnel training – RAMS data assessment – Life Cycle Cost assessment – Performance review		

B.5 List of tools:

Some appropriate methods and tools for conducting and managing a RAMS programme are listed below. The choice of the relevant tool will depend on the system under consideration and the criticality, complexity, novelty, etc., of the system.

1. **An outline form of RAMS specification**: in order to assure assessment of all relevant RAMS requirements. (see annex A for an example).

2. **Procedures for formal design reviews:** with emphasis on RAMS, using some general and application specific check lists as appropriate. e.g.

IEC 61160 *Formal design review; (amendment 1)*

3. **Procedures for performing "top down" (deductive methods) and "bottom up" (inductive methods) preliminary, worst case and in-depth RAM analysis for simple and complex functional system structures**: an overview of commonly used RAM analysis procedures, methods, advantages and disadvantages, data input and other requirements for the various techniques is given in:

IEC 60300-3-1 *Dependability management — Part 3: Application guide - Section 1: Analysis techniques for dependability: Guide on methodology*

The various RAM analysis techniques are described in separate standards, some of these are as follows:

IEC 60706	*Guide on maintainability of equipment*
IEC 60706-1	*Part 1 — Sections 1, 2 and 3: Introduction, requirements and maintainability programme*
IEC 60706-2	*Part 2 — Section 5: Maintainability studies during the design phase*
IEC 60706-3	*Part 3 — Sections 6 and 7: Verification and collection, analysis and presentation of data*
IEC 60706-4	*Part 4 — Section 8: Maintenance and maintenance support planning*
IEC 60706-5	*Part 5 — Section 4: Diagnostic testing*
IEC 60706-6	*Part 6 — Section 9: Statistical methods in maintainability evaluation*
IEC 60812	*Analysis techniques for system reliability — Procedures for failure mode and effects analysis (FMEA)*
IEC 60863	*Presentation of reliability, maintainability and availability predictions*
IEC 61025	*Fault tree analysis (FTA)*
IEC 61078	*Analysis techniques for dependability — Reliability block diagram method*
IEC 61165	*Application of Markov techniques*

Availability of supportable statistical "RAM" data, for the components used in a design, (typically: failure rates, repair rates, maintenance data, failure modes, event rates, distribution of data and random events, etc.) is fundamental to RAM analysis. e.g.

IEC 61709 (1996)	*Electronic components — Reliability — Reference conditions for failure stress models for conversion rate and*
US MIL HDBK 217	*Reliability Prediction for Electronic Systems*

A number of computer programmes for system RAM analysis and statistical data analysis are also available.

4. **Procedures for performing hazard & safety/risk analysis.** Some of these are described in:

US MIL HDBK 882C	*System safety programme requirements*
US MIL HDBK 764 (MI)	*System safety engineering, design guide for army material*

The same basic techniques and analysis methods listed for RAM (item 3), are also applicable for safety/risk analysis.

Also see IEC 61508, Parts 1-7, under the general title "Functional safety of electrical/electronic/programmable electronic safety-related systems", consisting of the following parts:

- Part 1: General requirements;
- Part 2: Requirements for electrical/electronic/programmable electronic systems;
- Part 3: Software requirements;
- Part 4: Definitions and abbreviations;
- Part 5: Examples of methods for the determination of safety integrity levels;
- Part 6: Guidelines on the application of Parts 2 and 3;
- Part 7: Overview of techniques and measures.

5. **RAMS testing plans and procedures:** in order to test the long-term operating behaviour of components, equipment or systems and to demonstrate compliance with the requirements. Furthermore RAMS analysis and test results are used to devise RAMS improvement programmes, e.g.

IEC 60605:	*Equipment reliability testing*
IEC 60605-1 + A1	*Part 1: General requirements*
IEC 60605-2	*Part 2: Design of test cycles*
IEC 60605-3-1	*Part 3: Preferred test conditions. Indoor portable equipment - Low degree of simulation*
IEC 60605-3-2	*Part 3: Preferred test conditions - Equipment for stationary use in weatherprotected locations - High degree of simulation*
IEC 60605-3-3	*Part 3: Preferred test conditions - Section 3: Test cycle 3: Equipment for stationary use in partially weatherprotected locations - Low degree of simulation*
IEC 60605-3-4	*Part 3: Preferred test conditions - Section 4: Test cycle 4: Equipment for portable and non-stationary use - Low degree of simulation*
IEC 60605-4 + A1	*Part 4: Procedure for determining point estimates and confidence limits for equipment reliability determination test*
IEC 60605-6	*Part 6: Tests for the validity of the constant failure rate or constant failure intensity assumptions*
IEC 61014	*Programmes for reliability growth*
IEC 61070	*Compliance test procedure for steady-state availability*
IEC 61123	*Reliability testing - Compliance test plan for success ratio*

Of greater importance is the **assessment of RAMS data from the field** (RAMS testing during operation), e.g.:

IEC 60300-3-2	*Dependability management — Part 3: Application guide — Section 2: dependability data from the field*
IEC 60319	*Presentation of reliability data on electronic components (or parts)*

6. **Procedures/tools to perform LCC analysis** (Life Cycle Cost): various computer programmes are available for LCC analysis

Annex C (informative)

Examples of parameters for railway

Examples of typical parameters and symbols, suitable for use in railway applications, are tabulated below:

C.1 Reliability parameters:

Table C.1 — Examples of Reliability Parameters

PARAMETER	SYMBOL	DIMENSION
Failure Rate	$Z(t)$, λ	failures / time, distance, cycle
Mean Up Time	MUT	time, distance, cycle
Mean Time To Failure Mean Distance To Failure (for non-repairable items)	MTTF MDTF	time, distance, cycle
Mean Time Between Failure Mean Distance Between Failure (for repairable items)	MTBF MDBF	time, distance, cycle
Failure Probability	$F(t)$	dimensionless
Reliability (Success Probability)	$R(t)$	dimensionless

C.2 Maintainability parameters:

Table C.2 — Examples of Maintainability Parameters

PARAMETER	SYMBOL	DIMENSION
Mean Down Time	MDT	time, distance, cycle
Mean Time/Distance Between Maintenance	MTBM/MDBM	time, distance, cycles
MTBM/MDBM, Corrective or Preventive	MTBM(c)/MDBM(c), MTBM(p)/MDBM(p)	time, distance, cycles
Mean Time To Maintain	MTTM	time
MTTM, Corrective or Preventive	MTTM(c), MTTM(p)	time
Mean Time To Restore	MTTR	time
False Alarm Rate	FAR	$time^{-1}$
Fault Coverage	FC	dimensionless
Repair Coverage	RC	dimensionless

C.3 Availability parameters:

Table C.3 — Examples of Availability Parameters

PARAMETER	SYMBOL	DIMENSION
Availability inherent achieved operational	A (.) = MUT/(MUT+MDT) A_i A_a A_o	 dimensionless
Fleet Availability	*FA* (= available vehicles/fleet)	dimensionless
Schedule Adherence	*SA*	dimensionless

C.4 Logistic support parameters:

Table C.4 — Examples of Logistic Support Parameters

PARAMETER	SYMBOL	DIMENSION
Operation and Maintenance Cost	O&MC	money
Maintenance Cost	MC	money
Maintenance Man Hours	MMH	time (hours)
Logistic and Administrative Delay	LAD	time
Fault correction time		time
Repair time		time
Maintenance support performance		dimensionless
Employees for Replacement	EFR	dimensionless
Probability of Spare Parts on Stock when needed	SPS	dimensionless

C.5 Safety parameters:

Table C.5 — Examples of Safety Performance

PARAMETER	SYMBOL	DIMENSION
Mean Time Between Hazardous Failure	MTBF(H)	time, distance, cycle
Mean Time Between "Safety System Failure"	MTBSF	time, distance, cycle
Hazard Rate	$H(t)$	failures/time, distance, cycle
Safety Related Failure Probability	$F_S(t)$	dimensionless
Probability of Safe Functionality	$S_S(t)$	dimensionless
Time to Return to Safety	TTRS	time

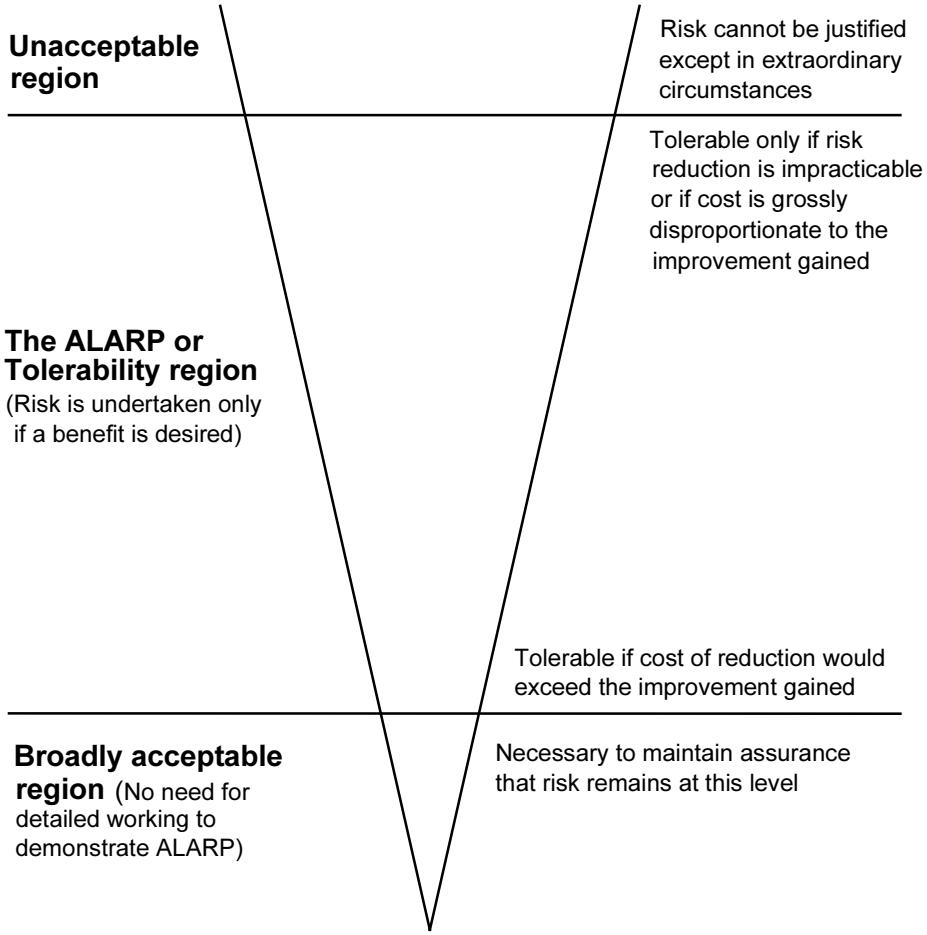
Annex D (informative)

Examples of some risk acceptance principles

NOTE: Values given in this annex are only to illustrate the principles and are not intended to be used for any other purpose.

D.1 As Low As Reasonably Practicable (ALARP) principle (practised in UK)

The principle may be represented by the following diagram:



D.1.1 Some risks are so large and some outcomes so unacceptable that they are intolerable and cannot be justified on any grounds. The upper bound defines levels of risk that are intolerable. If the level of risk cannot be reduced below this bound then the operation should not be carried out.

D.1.2 The lower bound of the diagram defines the broadly acceptable region where risks are considered to be so low that strenuous efforts to reduce them further would not be likely to be justified by any ALARP criteria.

D.1.3 The area between the upper and lower bounds is called the ALARP region. It must be stressed that it is not sufficient to demonstrate that risks are in the ALARP region. They must be made as low as reasonably practicable. There are various ways to demonstrate ALARP. It may be sufficient to show that the best available current standards and practices are being applied. For novel operations, or where the adequacy of current standards or practices are in doubt, the concepts of cost benefit analysis and value of life can be introduced.

D.1.4 Societal risk has to be examined when there is the possibility of a catastrophe involving large number of casualties. The dislike of large accidents is termed "Differential Risk Aversion" (DRA). This may be expressed by a slope of (-1) in the log *F-N* curve, where *F* is the frequency of occurrence (year -1) and *N* the number of casualties for an occurrence.

D.2 Globalement Au Moins Aussi Bon (GAMAB) principle (practised in France)

The complete formulation of this principle is as follows:
"All new guided transport systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system".

D.2.1 This formulation takes into account what has been done and requires implicitly a progress to be made in the projected system, by the requirement "at least". It does not consider a particular risk, by the requirement "globally". The transport system supplier is free to distribute allocation between the different risks inherent to the system and applies the relevant approach, i.e. qualitative or quantitative.

D.2.2 When a quantitative approach is applied, it may be translated in the following way:

1. Let $\tau_{c.ref}$ be the fraction (casualty/passenger) experienced for a certain number of transported passengers by a transport system in the last years of operation, casualties caused by collision between two trains. This fraction should be extracted from the statistics for the existing system and form the reference for the new system, of the same nature.

2. Now consider the new (replacement) system. For this system let:

   C = capacity of one train (passengers/train)
   F = frequency of trains (trains/hour)
   r = mean occupation coefficient (train not completely full)
   n_c = number of casualties per collision in this new system
   D_m = throughput (passengers/hour) = $r*C*F$

Therefore, the number of collisions actually seen by each passenger(col), must be:
col = $(\tau_{c.ref} / n_c) * $ (collision/passenger)

Also the collision rate for the new system must be smaller than that of the existing system:

Therefore,

$$\begin{aligned} \lambda_c &\leq \text{col} * D_m \\ &= (\tau_{c.ref} / n_c) * D_m \\ &= \tau_{c.ref} * (r*C / n_c) * F \text{ collision/hour} \end{aligned}$$

3. Remarks:

It is assumed that the proportion of casualties among the passengers in the same train is the same for the exiting system and the projected system:

- i.e. $n_c / r*C$ = constant;
- λ_c can be a tough requirement for a poor quality of service, especially for low value of F (frequency of trains);
- Improvement is driven by the sign $\leq$;
- The designer/supplier is free to distribute λ_c between way-side equipment and on-board equipment.

D.3 Minimum Endogenous Mortality (MEM) principle (practised in Germany)

This principle has been derived in the following manner:

1. Death will result from many different causes. One such group of causes is termed "technological facts" e.g.

   — entertainment and sport (surf, trial, etc.);
   — do-it-yourself activities (lawn mowing, etc.);
   — work machines;
   — transport.

The following are not included:

   — death by illness or disease;
   — death by congenital malformation.

This group results in a certain percentage of death per annum that varies according to the age of the population being considered. This risk is referred to as "Endogenous Mortality" "R".

2. In well developed countries, R is the lowest for the age group 5 to 15 years. This lowest level of Endogenous Mortality, known as "Minimum Endogenous Mortality denoted by "R_m" has been determined as:

$R_m = 2 * 10^{-4}$ fatalities/person*year

3. From the above the following rule is formulated:

"Hazards due to a new system of transport would not significantly augment the figure R_m".

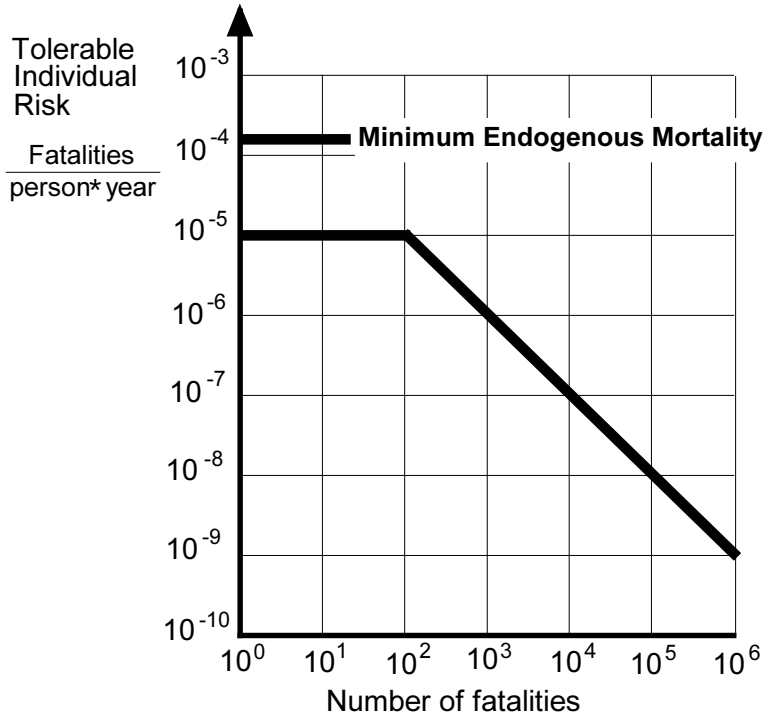
In practice the following figures may be used:

$R_1 \leq 10^{-5}$ fatality/person*year

$R_2 \leq 10^{-4}$ heavy injuries/person*year

$R_3 \leq 10^{-3}$ light injuries/person*year

This point of view is highly individualistic: the family of the person suffering the casualty will not find any solace in the fact that the person perished in a huge catastrophe or a small one. This is true as far as actual means of transport are concerned (train, plane, etc.). For systems that may result in large number of fatalities, "differential risk aversion" (DRA) is introduced by a decreasing slope as presented in the following curve:



Annex E (informative)

Responsibilities within the RAMS process throughout the lifecycle

As a general guideline, for a typical railway project, the following applies:

- Requirements are usually established by the customer or a regulatory (legal) authority.
- Approval and acceptance is similarly carried out by the customer or the regulatory authority.
- Solutions, their results and verifications are normally elaborated or performed by the contractor.
- Validation is normally performed jointly.

This general rule, however, depends on the contractual and legal relationship between the parties involved.
However, this standard requires that, in each case, the responsibilities for the tasks in the various lifecycle phases are defined and agreed. The following matrix gives an example of responsibilities for a typical arrangement.

	Customer/ Operator	Approval Authority	(Main) Contractor	Sub-Contractor	Suppliers
Concept Phase	**X**				
System Definition & Application Conditions	**X**				
Risk Analysis	**X**		**X**		
System Requirements	**X**	**(X)**			
Apportionment of System Requirements	**(X)**		**X**		
Design and Implementation			**X**	**(X)**	
Manufacture			**X**	**X**	**X**
Installation			**X**	**(X)**	
System Validation	**X**	**X**	**X**	**(X)**	
System acceptance	**X**	**X**			
Operation and Maintenance	**X**		**(X)**	**(X)**	
Performance Monitoring	**X**		**(X)**	**(X)**	
Modification and Retrofit	**X**		**X**	**X**	
De-commissioning and Disposal	**X**		**(X)**		

Where,
X full responsibility and participation
(X) specific responsibility and/or partial participation (e.g. on sub-contract or on standby basis)

blank

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: 020 8996 9000. Fax: 020 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: 020 8996 9001. Fax: 020 8996 7001.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: 020 8996 7111. Fax: 020 8996 7048.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: 020 8996 7002. Fax: 020 8996 7001.

Copyright

BSI
389 Chiswick High Road
London
W4 4AL