BS EN 50126-1:2017

BSI Standards Publication

Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

Part 1: Generic RAMS Process

bsi.

National foreword

This British Standard is the UK implementation of EN 50126-1:2017. It supersedes BS EN 50126-1:1999, which is withdrawn.

This standards series represents a significant change from BS EN 50126:1999 and the UK Committee acknowledges the efforts and progress made. However, the UK committee is of the opinion that a majority of UK comments have not been incorporated. Consequently, the UK recommends users read the requirements carefully in order to understand the standards correctly, particularly in fields of application and aspects of RAMS where EN 50126 may not have been applied historically.

The UK participation in its preparation was entrusted to Technical Committee GEL/9, Railway Electrotechnical Applications.

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

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2017

ISBN 978 0 580 91692 2

ICS 45.020; 29.280

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2017.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50126-1

October 2017

ICS 29.280; 45.020

Supersedes EN 50126-1:1999

English Version

Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 1: Processus FMDS générique

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 1: Generischer RAMS Prozess

This European Standard was approved by CENELEC on 2017-07-03. 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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 50126-1:2017 E

Contents

Page

European foreword 6
Introduction 7
1 Scope 8
2 Normative references 9
3 Terms and definitions 9
4 Abbreviations 20
5 Railway RAMS 20
5.1 Introduction 20
5.2 Multi-level System approach 21
5.2.1 Concepts of system hierarchy 21
5.2.2 System requirements and characteristics 22
5.2.3 Defining a system 23
5.3 Railway system overview 23
5.3.1 Introduction 23
5.3.2 Stakeholders involved in a railway system 23
5.3.3 Railway system structure and apportionment of RAMS requirements 24
5.4 Railway RAMS and quality of service 24
5.5 Elements of railway RAMS 24
5.6 Factors influencing railway RAMS 27
5.6.1 General 27
5.6.2 Classes of failures 27
5.6.3 Derivation of detailed railway specific influencing factors 27
5.6.4 Human factors 32
5.7 Specification of railway RAMS requirements 34
5.7.1 General 34
5.7.2 RAMS specification 34
5.8 Risk based approach 34
5.9 Risk reduction strategy 35
5.9.1 Introduction 35
5.9.2 Reduction of risks related to safety 35
5.9.3 Reduction of risks related to RAM 36
6 Management of railway RAMS – general requirements 37
6.1 Introduction 37
6.2 Life cycle for the system under consideration 37
6.3 Risk assessment 45
6.4 Organisational requirements 46
6.4.1 Introduction 46
6.4.2 Requirements 47
6.5 Application of this standard and adaptability to project scope and size 47
6.5.1 General requirements 47
6.5.2 Case of complex systems with different hierarchical levels 49
6.5.3 Renewal within existing systems 50

6.5.4 Re-use or adaptation of a system with previous acceptance 50
6.6 General requirements on RAMS documentation 51
6.7 Verification and Validation 52
6.7.1 Introduction 52
6.7.2 Verification 52
6.7.3 Validation 52
6.8 Independent Safety Assessment 53
6.8.1 Objectives 53
6.8.2 Activities 54
7 RAMS life cycle 55
7.1 General 55
7.2 Phase 1: Concept 55
7.2.1 Objectives 55
7.2.2 Activities 56
7.2.3 Deliverables 56
7.3 Phase 2: System definition and operational context 56
7.3.1 Objectives 56
7.3.2 Activities 56
7.3.3 Deliverables 60
7.4 Phase 3: Risk analysis and evaluation 60
7.4.1 Objectives 60
7.4.2 Activities 61
7.4.3 Deliverables 64
7.5 Phase 4: Specification of system requirements 64
7.5.1 Objectives 64
7.5.2 Activities 65
7.5.3 Deliverables 66
7.5.4 Specific validation tasks 66
7.6 Phase 5: Architecture and apportionment of system requirements 67
7.6.1 Objectives 67
7.6.2 Activities 67
7.6.3 Deliverables 68
7.7 Phase 6: Design and Implementation 68
7.7.1 Objectives 68
7.7.2 Activities 68
7.7.3 Deliverables 69
7.7.4 Specific verification tasks 70
7.8 Phase 7: Manufacture 70
7.8.1 Objectives 70
7.8.2 Activities 70
7.8.3 Deliverables 71
7.9 Phase 8: Integration 71
7.9.1 Objectives 71
7.9.2 Activities 71
7.9.3 Deliverables 72
7.9.4 Specific verification tasks 72
7.10 Phase 9: System Validation 73
7.10.1 Objectives 73

7.10.2 Activities 73
7.10.3 Deliverables 73
7.11 Phase 10: System acceptance 74
7.11.1 Objectives 74
7.11.2 Activities 75
7.11.3 Deliverables 75
7.12 Phase 11: Operation, maintenance and performance monitoring 75
7.12.1 Objectives 75
7.12.2 Activities 75
7.12.3 Deliverables 78
7.12.4 Specific verification tasks 79
7.13 Phase 12: Decommissioning 79
7.13.1 Objectives 79
7.13.2 Activities 79
7.13.3 Deliverables 79
8 Safety Case 79
8.1 Purpose of a safety case 79
8.2 Content of a safety case 80
Annex A (informative) RAMS plan 82
A.1 General 82
A.2 Procedure 82
A.3 Basic RAMS plan example 82
A.4 List of techniques 84
Annex B (informative) Examples of parameters for railway 86
B.1 General 86
B.2 Reliability parameters 86
B.3 Maintainability parameters 86
B.4 Availability parameters 87
B.5 Logistic support parameters 89
B.6 Safety parameters 89
Annex C (informative) Risk matrix calibration and risk acceptance categories 90
C.1 General 90
C.2 Frequency of occurrence categories 90
C.3 Severity categories 92
C.4 Risk acceptance categories 93
Annex D (informative) Guidance on system definition 95
D.1 General 95
D.2 System Definition in an iterative system approach 95
D.3 Method for defining the structure of a system 95
D.3.1 General 95
D.3.2 Function List 95
D.3.3 Functional breakdown 95
D.4 Parties/stakeholders/boundaries of systems 96
D.5 Guidance on the content of a system definition 96

Annex ZZ (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 2008/57/EC 98
Bibliography 102

Table 1 — RAMS tasks along life-cycle phases (1 of 4) 41
Table A.1 – Example of a basic RAMS plan outline (part 1 of 2) 83
Table B.1 – Examples of reliability parameters 86
Table B.2 – Examples of maintainability parameters 86
Table B.3 – Examples of availability parameters 87
Table B.4 – Examples of logistic support parameters 90
Table B.5 – Examples of safety performance parameters 90
Table C.1 – Frequency of occurrence of hazardous events with examples for quantification (time based) 91
Table C.2 – Frequency of occurrence of events with examples for quantification (distance based) 92
Table C.3 – Severity categories (example related to RAM) 93
Table C.4 – Severity categories (example 1 related to RAMS) 93
Table C.5 – Severity categories (example 2 related to Safety) 94
Table C.6 – Financial severity categories (example) 94
Table C.7 – Risk acceptance categories (example 1 for binary decisions) 94
Table C.8 – Risk acceptance categories (example 2) 94
Table C.9 – Risk acceptance categories (example related to safety) 95
Table D.1 – Typical examples for a functional breakdown 97

European foreword

This document (EN 50126-1:2017) has been prepared by CLC/TC 9X "Electrical and electronic applications for railways".

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2018-07-03
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2020-07-03

This document supersedes EN 50126-1:1999 which has been technically revised.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

EN 50126 "*Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*" consists of the following parts:

— Part 1: Generic RAMS process;

— Part 2: System approach to safety.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

For the relationship with EU Directive(s) see informative Annex ZZ, which is an integral part of this document.

Introduction

EN 50126-1:1999 was aimed at introducing the application of a systematic RAMS management process in the railway sector. Through the application of this standard and the experiences gained over the last years, the need for revision and restructuring became apparent with a need to deliver a systematic and coherent approach to RAMS applicable to all the railway application fields Command, Control and Signalling (Signalling), Rolling Stock and Electric power supply for Railways (Fixed Installations).

The revision work improved the coherency and consistency of the standard, the concept of safety management and the practical usage of EN 50126, and took into consideration the existing and related Technical Reports as well.

This European Standard provides railway duty holders and the railway suppliers, 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 promotes a common understanding and approach to the management of RAMS.

EN 50126 forms part of the railway sector specific application of IEC 61508. Meeting the requirements in this European Standard together with the requirements of other suitable standards is sufficient to ensure that additional compliance to IEC 61508 does not need to be demonstrated.

With regard to safety, EN 50126-1 provides a Safety Management Process which is supported by guidance and methods described in EN 50126-2.

EN 50126-1 and EN 50126-2 are independent from the technology used. As far as safety is concerned, EN 50126 takes the perspective of safety with a functional approach.

The application of this standard can be adapted to the specific requirements for the system under consideration.

This European Standard can be applied systematically by the railway duty holders and railway suppliers, throughout all phases of the life cycle of a railway application, to develop railway specific RAMS requirements and to achieve compliance with these requirements. The system-level approach developed by this European Standard facilitates assessment of the RAMS interactions between elements of railway applications even if they are of complex nature.

This European Standard promotes co-operation between the stakeholders of Railways 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.

In accordance with CENELEC editing rules [1)], mandatory requirements in this standard are indicated with the modal verb “shall”. Where justifiable, the standard permits process tailoring.

Specific guidance on the application of this standard for Safety aspects is provided in EN 50126-2. EN 50126-2 provides various methods for use in the safety management process. Where a particular method is selected for the system under consideration, the mandatory requirements for this method are by consequence mandatory for the safety management of the system under consideration.

This European Standard consists of the main part (Clause 1 to Clause 8) and Annexes A, B, C, D and ZZ. The requirements defined in the main part of the standard are normative, whilst Annexes are informative.

1) CEN/CENELEC Internal Regulations Part 3: Rules for the structure and drafting of CEN/CENELEC Publications (2017-02), Annex H.

1 Scope

This part 1 of EN 50126

- considers RAMS, understood as reliability, availability, maintainability and safety and their interaction;
- considers the generic aspects of the RAMS life cycle. The guidance in this part can still be used in the application of specific standards;
- defines:
  - a process, based on the system life cycle and tasks within it, for managing RAMS;
  - a systematic process, tailorable to the type and size of the system under consideration, for specifying requirements for RAMS and demonstrating that these requirements are achieved;
- addresses railway specifics;
- enables conflicts between RAMS elements to be controlled and managed effectively;
- does not define:
  - RAMS targets, quantities, requirements or solutions for specific railway applications;
  - rules or processes pertaining to the certification of railway products against the requirements of this standard;
  - an approval process for the railway stakeholders.

This part 1 of EN 50126 is applicable to railway application fields, namely Command, Control and Signalling, Rolling Stock and Fixed Installations, and specifically:

- to the specification and demonstration of RAMS for all railway applications and at all levels of such an application, as appropriate, from complete railway systems to major systems and to individual and combined subsystems and components within these major systems, including those containing software; in particular:
  - to new systems;
  - to new systems integrated into existing systems already accepted, but only to the extent and insofar as the new system with the new functionality is being integrated. It is otherwise not applicable to any unmodified aspects of the existing system;
  - as far as reasonably practicable, to modifications and extensions of existing systems already accepted, but only to the extent and insofar as existing systems are being modified. It is otherwise not applicable to any unmodified aspect of the existing system;
- at all relevant phases of the life cycle of an application;
- for use by railway duty holders and the railway suppliers.

It is not required to apply this standard to existing systems which remain unmodified, including those systems already compliant with any former version of EN 50126.

The process defined by this European Standard assumes that railway duty holders and railway suppliers 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 EN ISO 9001.

2 Normative references

Not applicable.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
acceptance
status achieved by a product, system or process once it has been agreed that it is suitable for its intended purpose

3.2
accident
unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage

[SOURCE: IEC 60050-821: FDIS2016, 821-12-02]

3.3
approval
permission for a product or process to be marketed or used for stated purposes or under stated conditions

Note 1 to entry: Approval can be based on fulfilment of specified requirements or completion of specified procedures.

[SOURCE: EN ISO/IEC 17000:2004, 7.1]

[SOURCE: IEC 60050-902:2013, 902-06-01]

3.4
assurance
confidence in achieving a goal being pursued. Declaration intended to give confidence

3.5
audit
systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled

Note 1 to entry: Whilst “audit” applies to management systems, “assessment” applies to conformity assessment bodies as well as more generally.

[SOURCE: EN ISO/IEC 17000:2004, 4.4, modified – The references to other terms within ISO/IEC 17000 have been replaced by hyperlinks to entries in the IEV.]

[SOURCE: IEC 60050-902:2013, 902-03-04]

3.6
availability, <of a product>
ability of an item 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

[SOURCE: IEC 60050-821: FDIS2016, 821-05-82, modified]

3.7
basic integrity
integrity attribute for safety related function with a TFFR higher than (less demanding) 10^{-5} [h^{-1}] or non-safety-related function.

3.8
collective risk
risk, resulting from e.g. a product, process or system, to which a population or group of people is exposed

Note 1 to entry: Collective risk is not to be confused with risk of multiple victim accident.

Note 2 to entry: Collective risk is the sum of the individual risks to those individuals in the population or group. However, the collective risk divided by the number of individuals will only provide the average individual risk.

Note 3 to entry: A group of people could be, for example, rail staff working in a restaurant car or all passengers using a particular network.

3.9
commercial off-the-shelf product
product defined by market-driven need, commercially available and whose fitness for purpose has been deemed acceptable by a broad spectrum of commercial users

[SOURCE: EN 50128:2011, 3.1.3, modified]

3.10
common cause failure
failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause

[SOURCE: IEC 60050-192:2015, 192-03-18]

3.11
compliance
state where a characteristic or property of a product, system or process satisfies the specified requirements

3.12
configuration management
process of identifying and documenting the characteristics of a facility's structures, systems and components (including computer systems and software), and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation

[SOURCE: IAEA 3, modified]

[SOURCE: IEC 60050-395:2014, 395-07-52]

3.13
consequence analysis
analysis of events which are likely to happen after a hazard has occurred

[SOURCE: IEC 60050-821: FDIS2016, 821-12-14]

3.14
corrective maintenance
maintenance carried out after fault detection to effect restoration

Note 1 to entry: Corrective maintenance of software invariably involves some modification.

[SOURCE: IEC 60050-192:2015, 192-06-06]

3.15
design
activity applied in order to analyse and transform specified requirements into acceptable solutions

[SOURCE: IEC 60050-821: FDIS2016, 821-12-16, modified]

3.16
deterministic
expresses that a behaviour can be predicted with certainty

Note 1 to entry: A deterministic event in a system can be predicted with certainty from preceding events which are either known or are the same as for a proven equivalent system.

3.17
diversity
existence of two or more different ways or means of achieving a specified objective

Note 1 to entry: Diversity is specifically provided as a defence against common cause failure. It can be achieved by providing systems that are physically different from each other or by functional diversity, where similar systems achieve the specified objective in different ways.

[SOURCE: IEC 60050-395:2014, 395-07-115]

3.18
entity
person, group or organisation who fulfils a role as defined in this standard

3.19
equivalent fatality
expression of fatalities and weighted injuries and a convention for combining injuries and fatalities into one figure for ease of evaluation and comparison of risks

3.20
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

Note 1 to entry: An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.

Note 2 to entry: A human error can be seen as a human action or inaction that can produce an unintended result.

[SOURCE: IEC 60050-192:2015, 192-03-02]

3.21
failure, <of an item>
loss of ability to perform as required

Note 1 to entry: Qualifiers, such as catastrophic, critical, major, minor, marginal and insignificant, may be used to categorize failures according to the severity of consequences, the choice and definitions of severity criteria depending upon the field of application.

Note 2 to entry: Qualifiers, such as misuse, mishandling and weakness, may be used to categorize failures according to the cause of failure.

[SOURCE: IEC 60050-192:2015, 192-03-01, modified Note 1 to entry has been omitted]

[SOURCE: IEC 60050-821:FDIS2016, 821-11-19]

Note 3 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

3.22
failure mode
manner in which failure occurs

[SOURCE: IEC 60050-192:2015, 192-03-17]

3.23
failure rate
limit 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 + Δt) and the duration 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

Note 1 to entry: For applications where distance travelled or number of cycles of operation is more relevant than time then the unit of time can be replaced by the unit of distance or cycles, as appropriate.

Note 2 to entry: The term “failure rate” is often used in the sense of “mean failure rate” defined in IEV 192-05-07.

[SOURCE: IEC 60050-821:FDIS2016]

3.24
fault, <in a system>
abnormal condition that could lead to an error in a system

Note 1 to entry: A fault can be random or systematic.

[SOURCE: IEC 60050-821:FDIS2016, 821-11-20]

3.25
function, <of an item>
specified action or activity which can be performed by technical means and/or human beings and has a defined output in response to a defined input

Note 1 to entry: A function can be specified or described without reference to the physical means of achieving it.

[SOURCE: IEC 60050-821:FDIS2016, 821-12-25, modified]

3.26
functional safety
part of the overall safety that depends on functional and physical units operating correctly in response to their inputs

[SOURCE: IEC 60050-351, 351-57-06]

3.27
generic product
product independent of applications, fulfilling predefined boundary conditions, interfaces and functionality (black box)

EXAMPLE: Examples point machines, axle counters, real-time operating systems, fail-safe computer platform without application software.

[SOURCE: IEC 60050-821:FDIS2016, 821-01-57]

3.28
hazard
condition that could lead to an accident

Note 1 to entry: The equivalent definition in [IEC 60050-903:2013, 903-01-02] refers to "harm" instead of "accident".

3.29
hazard analysis
process of identifying hazards and analysing their causes, and the derivation of requirements to limit the likelihood and consequences of hazards to a tolerable level

Note 1 to entry: Similar process aspects are also considered in risk assessment. In this standard the term is applied in life cycle phases after “requirements specification”.

[SOURCE: IEC 60050-821: FDIS2016, 821-11-23]

3.30
hazard log
document in which hazards identified, decisions made, solutions adopted and their implementation status are recorded or referenced

[SOURCE: IEC 60050-821:FDIS2016, 821-12-27]

3.31
hazard rate
rate of occurrence of a hazard

Note 1 to entry: For detailed mathematical understanding of "rate" refer to the definition of "failure rate".

3.32
implementation
activity applied in order to transform the specified designs into their realization

[SOURCE: IEC 60050-821:FDIS2016, 821-12-29, modified]

3.33
independent safety assessment
process to determine whether the system/product meets the specified safety requirements and to form a judgement as to whether the system/product is fit for its intended purpose in relation to safety

Note 1 to entry: Requirements for independence are defined in this European Standard.

3.34
individual risk
risk, resulting from e.g. a product, process or system, to which an individual person is exposed

Note 1 to entry: Individual risk is not to be confused with risk of single victim accidents.

Note 2 to entry: Collective risk is the sum of the individual risks to those individuals in the population or group. However, the collective risk divided by the number of individuals will only provide the average individual risk.

3.35
integration
process of assembling the elements of a system according to the architectural and design specification, and the testing of the integrated unit

3.36
life cycle
series of identifiable stages through which an item goes, from its conception to disposal

EXAMPLE A typical system lifecycle consists of: concept and definition; design and development; construction, installation and commissioning; operation and maintenance; mid-life upgrading, or life extension; and decommissioning and disposal.

Note 1 to entry: The stages identified will vary with the application.

Note 2 to entry: In case mid-life upgrading or life extension introduce changes, this standard requires re-consideration of the life cycle.

[SOURCE: IEC 60050-192:2015, 192-01-09]

3.37
maintainability, <of an item>
ability to be retained in, or restored to, a state to perform as required, under given conditions of use and maintenance

Note 1 to entry: Given conditions would include aspects that affect maintainability, such as: location for maintenance, accessibility, maintenance procedures and maintenance resources.

[SOURCE: IEC 60050-192:2015, 192-01-27]

3.38
maintenance
combination of all technical and management actions intended to retain an item in, or restore it to, a state in which it can perform as required

Note 1 to entry: Management is assumed to include supervision activities.

[SOURCE: IEC 60050-192:2015, 192-06-01]

3.39
mission
objective description of the fundamental task performed by a system

3.40
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 life cycle

3.41
negation
enforcement of a safe state following detection of a hazardous fault

[SOURCE: IEC 60050-821: FDIS2016, 821-12-38]

3.42
negation time
time interval which begins when the existence of a fault is detected and ends when a safe state is enforced

[SOURCE: IEC 60050-821: FDIS2016, 821-12-39]

3.43
pre-existing software
all software developed prior to the application currently in question is classed as pre-existing software including commercial off-the-shelf software, open-source software and software previously developed but not in accordance with this European Standard

3.44
preventive maintenance
maintenance carried out to mitigate degradation and reduce the probability of failure

Note 1 to entry: See also condition-based maintenance (192-06-07), and scheduled maintenance (192-06-12).

[SOURCE: IEC 60050-192:2015, 192-06-05]

3.45
product, <in railway>
collection of elements, interconnected to form a system, a subsystem or an equipment, in a manner which meets the specified requirements

[SOURCE: IEC 60050-821: FDIS2016, 821-12-40, specific use modified]

3.46
project management
administrative and/or technical conduct of a project, including RAMS aspects

3.47
project manager
entity that carries out project management

[SOURCE: EN 50128:2011, 3.1.21]

3.48
railway duty holder
body with the overall accountability for operating a railway system within the legal framework

Note 1 to entry: Railway duty holder accountabilities for the overall system or its parts and life cycle 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.

Note 2 to entry: Typically the railway duty holders are railway undertakings and the infrastructure managers. Such splits are based on either statutory instruments or contractual agreements. Such responsibilities are defined at the earliest stages of a system life cycle.

3.49
RAM plan
documented set of time scheduled activities, resources and events serving to implement the organisational 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

3.50
RAMS management process
activities and procedures that are followed to enable the RAMS requirements for a product or an operation to be identified and met

Note 1 to entry: It provides a systematic and systemic approach to continually manage RAMS through the whole life cycle.

Note 2 to entry: This Process should be embedded in a management system at the organisational level.

Note 3 to entry: Each means of accomplishing the function need not necessarily be identical.

3.51
random failure
unpredictable failure which results from one or more of the possible degradation mechanisms

3.52
reliability, <of an item>
ability to perform as required, without failure, for a given time interval, under given conditions

Note 1 to entry: The time interval duration can be expressed in units appropriate to the item concerned, e.g. calendar time, operating cycles, distance run, etc.

Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.

Note 3 to entry: Reliability can be quantified using measures defined in Section 192-05, Reliability related concepts: measures.

[SOURCE: IEC 60050-192:2015, 192-01-24]

3.53
reliability growth, <of an item>
iterative process for reliability improvement

[SOURCE: IEC 60050-192:2015, 192-12-03, modified]

3.54
repair
direct action taken to effect restoration

Note 1 to entry: Repair includes fault localisation (SOURCE: IEC 60050-192:2015, 192-06-19), fault diagnosis (SOURCE: IEC 60050-192:2015, 192-06-20), fault correction (SOURCE: IEC 60050-192:2015, 192-06-21) and function checkout (SOURCE: IEC 60050-192:2015, 192-06-22).

[SOURCE: IEC 60050-192:2015, 192-06-14]

3.55
residual risk
risk remaining after risk control measures have been taken

[SOURCE: IEC 60050-903:2013, 903-01-11]

3.56
restoration
bringing an item into a state where it regains the ability to perform its required function after a fault

3.57
risk, <for railway RAMS>
combination of expected frequency of loss and the expected degree of severity of that loss

3.58
risk analysis
systematic use of available information to identify hazards and to estimate the risk

[SOURCE: ISO/IEC Guide 51:2014, 3.10]

[SOURCE: IEC 60050-903:2013, 903-01-08]

3.59
risk assessment
overall process comprising a risk analysis and a risk evaluation

[SOURCE: ISO/IEC Guide 51:2014, 3.12]

[SOURCE: IEC 60050-903:2013, 903-01-10]**.**

3.60
risk based approach
process for ensuring the safety of products, processes and systems through consideration of the hazards and their consequent risks

Note 1 to entry: The approach is applicable to RAM aspects in an analogous manner.

3.61
risk evaluation
procedure based on the risk analysis to determine whether the tolerable risk has been achieved

[SOURCE: ISO/IEC Guide 51:2014, 3.11]

[SOURCE: IEC 60050-903:2013, 903-01-09]

3.62
risk management
systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risk

3.63
safe state
condition which continues to preserve safety

[SOURCE: IEC 60050-821: FDIS2016, 821-12-50]

3.64
safety
freedom from unacceptable risk

Note 1 to entry: Risk related to human health or to the environment.

[SOURCE: IEC 60050-903:2013, 903-01-19]

3.65
safety authority
body responsible for delivering the authorization for the operation of the safety-related system

[SOURCE: IEC 60050-821:FDIS2016, 821-12-52]

3.66
safety barrier
physical or non-physical means, which reduces the frequency of a hazard and/or a likely accident arising from the hazard and/or mitigates the severity of likely accidents arising from the hazard

Note 1 to entry: This term can be applied to RAM aspects in a similar manner.

3.67
safety case
documented demonstration that the product (e.g. a system, subsystem or equipment) complies with the specified safety requirements

[SOURCE: IEC 60050-821: FDIS2016, 821-12-53]

3.68
safety function
function whose sole purpose is to ensure safety

Note 1 to entry: A safety-related function is a function whose failure affects safety (for details refer to definition of "safety-related"). Therefore, all safety functions are safety-related functions, but not vice versa.

Note 2 to entry: A safety function may contribute to one or more safety barriers. However, a safety barrier is not necessarily implemented by a safety function.

3.69
safety integrity
ability of a safety-related system to achieve its required safety functions under all the stated conditions within a stated operational environment and within a stated duration

[SOURCE: IEC 60050-821:FDIS2016, 821-12-54]

3.70
safety integrity level
one of a number of defined discrete levels for specifying the safety integrity requirements for safety-related functions to be allocated to the safety-related systems

Note 1 to entry: Safety Integrity Level with the highest figure has the highest level of safety integrity.

Note 2 to entry: It is not possible to allocate a Safety Integrity Level to safety-related processes or other measures.

3.71
safety management
management structure which ensures that the safety process is properly implemented

3.72
safety management process
part of the RAMS management process which deals specifically with safety aspects

3.73
safety plan
documented set of time scheduled activities, resources and events serving to implement the organization, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given safety requirements relevant to a given contract or project

[SOURCE: IEC 60050-821:FDIS2016, 821-12-57]

3.74
safety-related
carries responsibility for safety

Note 1 to entry: A function, component, product, system or procedure is called safety-related if at least one of its properties is used in the safety argument for the system in which it is applied. These properties can be of functional or non-functional nature. The requirements attributed to the function can be systematic or random integrity requirements.

[SOURCE: IEC 60050-821: FDIS2016, 821-01-73, note 1 to entry added]

3.75
safety-related application conditions
those conditions which need to be met in order for a system to be safely integrated and safely operated

Note 1 to entry: Application conditions can for example be: operational restrictions (e.g. speed limit, maximum duration of use), operational rules, maintenance restrictions (e.g. requested maintenance intervals) or environmental conditions.

3.76
software
intellectual creation comprising the programs, procedures, rules, data and any associated documentation pertaining to the operation of a system

Note 1 to entry: The software baseline will enable the organisation to reproduce defined versions and be the input for future releases at enhancements or at upgrade in the maintenance phase.

[SOURCE: IEC 60050-192:2015, 192-01-07, modified]

3.77
subsystem
part of a system, which is itself a system

[SOURCE: IEC 60050-192:2015, 192-01-04]

3.78
system
set of interrelated elements considered in a defined context as a whole and separated from their environment

[SOURCE: IEC 60050-351:2013, 351-42-08]

3.79
systematic failure
failure that consistently occurs under particular conditions of handling, storage or use

Note 1 to entry: A systematic failure can be reproduced by deliberately applying the same conditions, although not all reproducible failures are systematic.

Note 2 to entry: The cause of a systematic failure originates in the specification, design, manufacture, installation, operation or maintenance of the item.

[SOURCE: IEC 60050-192:2015, 192-03-10]

3.80
technical safety
part of safety that is dependent upon the characteristics of a product, which derive from the system functional requirements and/or of the system design

3.81
testing
determination of one or more characteristics of an object of conformity assessment, according to a procedure

Note 1 to entry: “Testing” typically applies to materials, products or processes.

[SOURCE: IEC 60050-902:2013, 902-03-02]

3.82
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

Note 1 to entry: The term “validated” is used to designate the corresponding status.

Note 2 to entry: The use conditions for validation can be real or simulated.

Note 3 to entry: In design and development, validation concerns the process of examining an item to determine conformity with user needs.

Note 4 to entry: Validation is normally performed during the final stage of development, under defined operating conditions, although it can also be performed in earlier stages.

Note 5 to entry: Multiple validations can be carried out if there are different intended uses.

[SOURCE: IEC 60050-192:2015, 192-01-18]

3.83
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: The term “verified” is used to designate the corresponding status.

Note 2 to entry: Design verification is the application of tests and appraisals to assess conformity of a design to the specified requirement.

Note 3 to entry: Verification is conducted at various life cycle phases of development, examining the system and its constituents to determine conformity to the requirements specified at the beginning of that life cycle phase.

[SOURCE: IEC 60050-192:2015, 192-01-17, note 3 to entry modified]

4 Abbreviations

CoP	Code of Practice
COTS	Commercial Off-The-Shelf
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FC	Fault Coverage
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FRACAS	Failure Reporting Analysis and Corrective Action System
FTA	Fault Tree Analysis
LAD	Logistic and Administrative Delay
LCC	Life cycle Cost
MDT	Mean Down Time
MTBF	Mean Time Between Failures
MTBM	Mean Time Between Maintenances
MTTF	Mean Time To Failure
MUT	Mean Up Time
RAC	Risk Acceptance Criteria
RAM	Reliability, availability and maintainability
RAMS	Reliability, availability, maintainability and safety
RC	Repair Coverage
SRAC	Safety-Related Application Conditions
TFFR	Tolerable Functional Failure Rate
THR	Tolerable Hazard Rate

5 Railway RAMS

5.1 Introduction

This clause is intended to outline the body of knowledge on the subject of RAMS needed to enable users of the standard to fully understand what is required to comply in an appropriate way with the provisions of the normative text throughout the standard.

The objective of the RAMS process described in this standard is to ensure that all aspects of RAMS are covered in order to make provision for the safety of railway applications and for the avoidance of loss of their value.

Safety and avoidance of loss of value of the service are achieved most effectively when RAMS factors are continuously controlled throughout a project from its inception through to operation instead of adding on corrective systems in later stages.

This European Standard defines a management process, based on a system life cycle, which will enable the control of RAMS factors specific to railway applications. This RAMS management process is described in the next sub-clauses, where sub-clauses 5.6 to 5.8 contain requirements. Detailed requirements are provided in Clause 6.

Railway RAMS is a major contributor to the value of the service provided by railway duty holder. Railway RAMS is defined by several contributory elements; consequently, this clause is structured as follows:

a) sub-clauses 5.2 and 5.3 provide an overview of the systems approach and system definition within the context of railways;

b) sub-clause 5.4 examines the relationship between railway RAMS and the value of the service provided;

c) sub-clause 5.5 outlines the railway RAMS elements and their interactions;

d) sub-clauses 5.6 to 5.9 examine aspects of railway RAMS, namely:

– the factors which influence and means to achieve RAMS targets,

– specification of RAMS requirements,

– risk and safety integrity.

5.2 Multi-level System approach

5.2.1 Concepts of system hierarchy

Within this standard, the sequence “system, subsystem, component” is used to demonstrate the breakdown of a system into its constituent parts. The precise boundary of each element (system, subsystem and component), either physical or functional, will depend upon the design of the system in question. The system itself is contained in an operational environment.

The behaviour and state of the system might change if there is a change to the functionality or interaction of a subsystem or component. A system responds to inputs to produce specified outputs, whilst interacting with an environment.

The use of the terms system and subsystem can depend on the point of view taken. Something which is regarded as a system by the people who developed it might be regarded as a subsystem by people who use it as part of their system. This difference of points of view is rationalised by the concept of nested systems in a system hierarchy as shown diagrammatically by Figure 1.

According to the nested systems concept, systems are themselves built up of smaller systems that themselves are built up of even smaller systems and so on.

For convenience, multi level nested systems are usually handled on the basis of groupings of systems at successive levels of a hierarchy. The example in Figure 1 is a three level hierarchy consisting of a “system under consideration” (subsystem D) containing intra-related subsystems and / or components (W, X, Y and Z) and itself being contained, together with its inter-related subsystems and / or components (A, B and C) in a containing or parent system (e.g. braking system, signalling system or even the railway system as a whole). This provides visibility of the three levels and enables consideration of:

– the interactions and interfaces between the “system under consideration” and its “siblings” i.e. the inter-related subsystems / components, and

– the influences and interactions between the “system under consideration” and its environment (i.e. the “parent” or “containing system”).

Functions of a system are the actions or activities performed by the system as a whole. Functions and structure provide the “internal” view of the system properties that produce the outputs and external properties and are the concern of the body/entity responsible for the design of the system. The environment consists of anything that could influence, or be influenced by, the system. This will include anything to which the system connects mechanically, electrically or by other means, including EMI, thermal stress, etc. The environment will also include people and procedures that can affect, or be affected by, the operation of the system.

Understanding the boundary between the system under consideration and its environment and the interactions with its inter-related subsystems is a pre-requisite to understanding how failures of the system might contribute to an accident and what its hazards are.

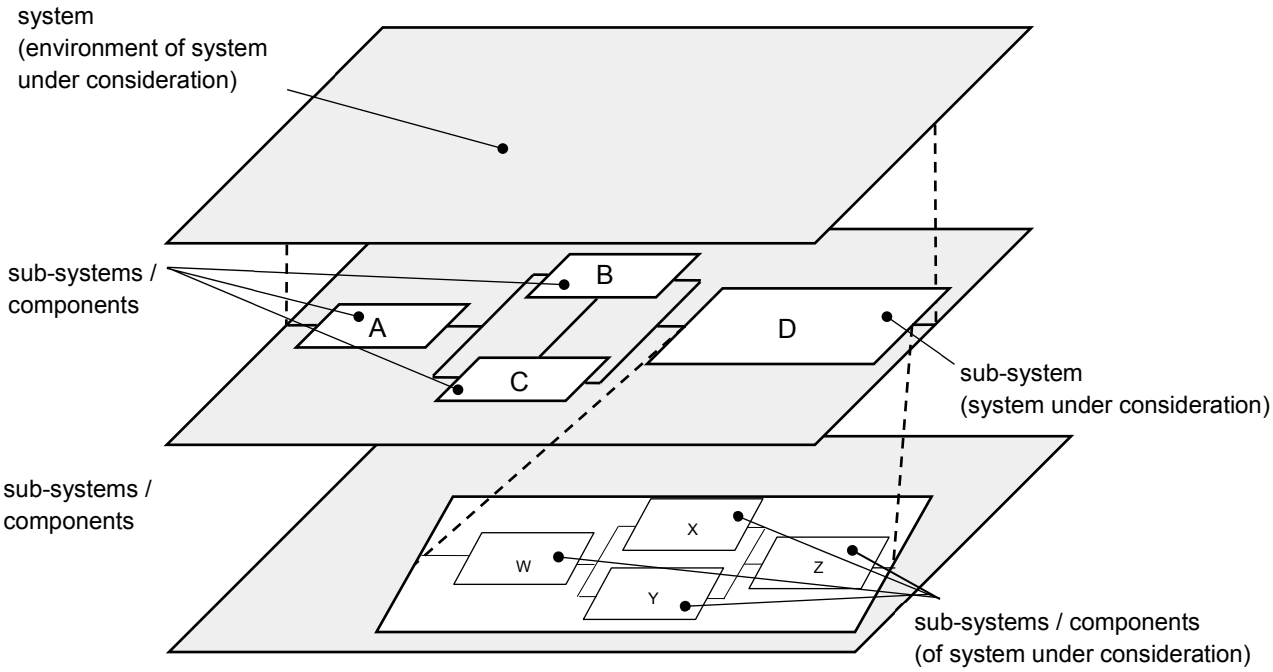


Figure 1 — Illustration of system hierarchy

5.2.2 System requirements and characteristics

System requirements are elicited from various sources. Requirements can be categorised, but a unique and unambiguous categorisation is not possible. Therefore, the following classification is for purposes of illustration:

– Functional requirements: a system is implemented to fulfil certain functions that are fundamental to the system and the prime reason for its creation. Depending on the system design, additional requirements might also be needed to ensure proper functioning of the system. The fundamental requirements and the additional requirements together are referred to as “Functional requirements”. They express the behaviour of the system and might also need to be complemented by properties qualifying its behaviour (e.g. reliability, safety, accuracy, timing, etc.) and by performance requirements expressed in terms of boundary values of functional parameters (e.g. maximum speed, service duration, response time, accuracy, etc.).

– Contextual requirements: the relation between the system and its environment might need to be further qualified by means of contextual requirements. They would address issues like the system mission profile, maintenance and logistics, human factors (e.g. personal qualification), procedural environment, costs, etc.

– Technical requirements: the technical implementation of the system can generate further requirements that do not derive from the system functions but from its technical implementation. Such requirements are referred to as “Technical requirements”. They impact the system build. Technical requirements might address issues such as maintainability, environmental conditions, potential threats created by the technology/ equipment regardless of their intended functions (e.g. presence of sharp edges, presence of electric voltage, presence of combustible material, etc.).

Detailed design involves engineering of the subsystems and equipment that implement the requirements for the system under consideration. It leads to the refining of the requirements in order to ensure compatibility between the different subsystems / equipment, and to the implementation of the refined requirements ensuring coherence with the technical and contextual requirements.

5.2.3 Defining a system

A system comprises not only its technical components but also the interaction with the humans developing, operating, and maintaining it. Therefore, it is the objective of the activities specified in 7.3.2 to ensure that these interactions are included in the definition and documentation of the system, taking into account the concept of system hierarchy explained in 5.2.

Further guidance on system definition is given in Annex D.

5.3 Railway system overview

5.3.1 Introduction

Subclause 5.3 gives a perspective of the railway system, the stakeholders involved in it and on some of the underlying concepts and RAMS considerations (e.g. risk, hazards). An understanding of the system and its elements is essential for the management of railway RAMS.

5.3.2 Stakeholders involved in a railway system

Depending on the social/political environment and the organisational /management structure of the railway system concerned, a number of stakeholders, performing different functions, can be involved within the life cycle phases of the system. For the purpose of this standard the stakeholders are divided into the following main categories:

- railway undertakings (railway duty holder);
- infrastructure managers (railway duty holder);
- maintainers;
- railway supply industry;
- safety authorities.

As far as the RAMS process is concerned, when developing products before a customer has been identified, the railway supply industry might need to undertake some of the functions of a railway duty holder.

The roles and responsibilities of these stakeholders can be contracted out to several other stakeholders or sub-contractors, depending on:

- social, political or legal considerations;
- size and complexity of the system or subsystem concerned;
- economic, organisational or managerial considerations.

It is therefore advisable to identify all the stakeholders that can be a part of this relationship and to examine and document how the roles and responsibilities of dealing with RAMS, during the life cycle of the system/subsystem concerned, are shared between them.

The railway duty holders bear the primary responsibility for assessing, controlling and reducing risk. For this task it can be necessary to obtain the relevant RAMS related information from the railway suppliers about the products involved.

NOTE As an illustration, the following might apply for a railway project with the potential to affect safety:

- requirements are usually established by the railway duty holder and/or a safety (legal) authority. These are usually functional requirements;
- requirements coming from the products (e.g. because of technology used) are usually established by the railway suppliers;
- safety approval is carried out either by the safety authority or by the railway duty holder depending on the relevant legal framework;
- acceptance of RAM is carried out by the railway duty holder;
- solutions, their results and verifications are normally elaborated or performed by the railway supplier;
- validation normally involves both the railway duty holder and the railway supplier.

Requirements relating to roles and responsibilities are given in 6.4.

5.3.3 Railway system structure and apportionment of RAMS requirements

The railway system, as with any system, can be viewed from a physical or functional perspective. No single view or breakdown of the system will suit all needs, and the view ultimately adopted is dependent on the user and their requirements.

Based on the concept of system hierarchy (5.2), it would then be the task of the body/entity responsible for each of the subsystems to map or apportion the RAMS requirements to their subsystems/components. Defining precise boundaries and boundary conditions will support this apportionment. It is often helpful for this task to be carried out with the cooperation of the responsible body/entity of the subsystems/components to ensure that the requirements and targets are practicable. This process can require several iterations to ensure that the overall system is optimised.

A similar reference system can be considered to support this apportionment. In this case, all differences and the effect of these differences on the RAMS performance should be evaluated for acceptability. Differences can be functional, technical, environmental, operational or in the application context (e.g.: system boundaries and boundary conditions; maintenance and operational competence levels; functional and technical interfaces with its environment, especially with other systems).

5.4 Railway RAMS and quality of service

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 life cycle of the system. The RAMS of a system can be characterised as a qualitative and quantitative indicator of the degree that the system, or the subsystems and components comprising that system, can be relied upon to function as specified and to be both available and safe over a period of time. System RAMS, in the context of this European Standard, is a combination of the interrelated characteristics, reliability, availability, maintainability and safety.

The goal of a railway system is to achieve a defined level of rail traffic at a given time, safely and within certain cost limits. The Railway RAMS process determines the confidence with which the system can achieve 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.

RAM also has a significant effect on overall life cycle cost.

5.5 Elements of railway RAMS

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

The RAMS elements are interlinked in the sense that a weakness in any of them or mismanagement of conflicts between their requirements can prevent achievement of a dependable system. For example, a safety target can be achieved by ensuring the system enters a safe state (e.g. all trains stopped) in the event of a particular failure. The defined safe state can depend on operational/maintenance context (e.g. a train at standstill at platform rather than in tunnel). If there are circumstances where this safe state has a significant adverse impact on reliability/availability then a different and optimised solution might be needed in order to achieve the RAM targets without compromising safety.

Attainment of in-service availability targets will be achieved by optimising reliability & maintainability whilst considering the influence of maintaining safety. The related requirements can be met and controlled by a combination of design and implementation measures and through the ongoing, long term maintenance and operational activities, all according to the system environment.

Security characterises the resilience of a railway system to vandalism, malevolence and intentionally harmful human behaviour.

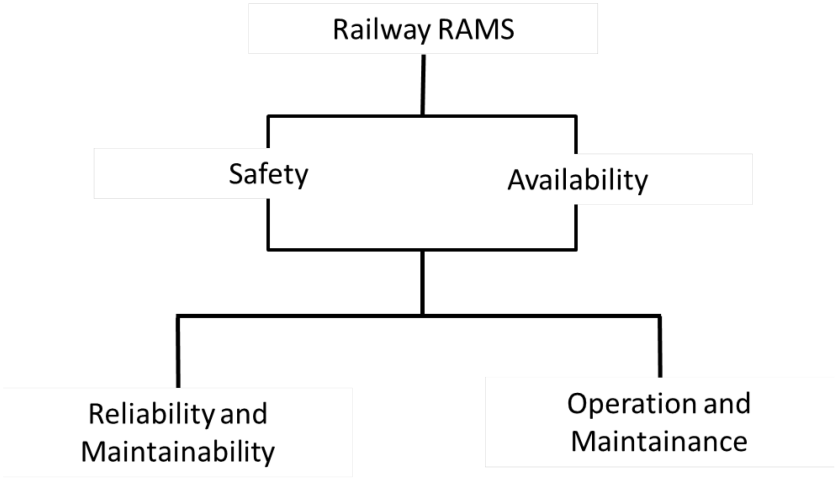


Figure 2 — Interrelation of railway RAMS elements

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 frequency of occurrence or the likelihood of each failure mode;

– the consequences of each failure mode.

b) maintainability in terms of:

– frequency and time for the performance of planned or unplanned maintenance;

– time for detection and identification 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 (taking into account cost issues), over the system life cycle;

– the human factor issues;

– tools, facilities and procedures for effective maintenance of the system.

Technical concepts of safety are based on a knowledge of:

d) all possible accidents and associated hazards that could result from a failure in the system, or from properties or characteristics of the system, under all operational, maintenance and environment modes;

e) the characteristics of each hazard;

f) safety-related failures in terms of:

– all system failure modes that could lead to a hazard (safety-related failure modes);

– the frequency of occurrence or the probability of each relevant safety-related system failure mode;

– sequence and/or coincidence of events, failures, operational states, environment conditions, etc., in the application, that can result in an accident (i.e. a hazard resulting in an accident);

– the frequency of occurrence or the probability of the relevant events, failures, operational states, environment conditions etc., in the application.

g) 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;

– possible errors occurring during maintenance actions on those safety-related parts of the system;

– time for restoring the system into a safe state.

h) system operation and maintenance of safety-related parts of the system in terms of:

– human factors influence on the maintenance and the operation;

– tools, facilities and procedures for effective maintenance of the system and for safe operation;

– effective controls and measures for dealing with a hazard and mitigating its consequences.

Failures in a system operating within the bounds of an application and environment will have an impact on the system's reliability, availability and safety, with the level of impact being determined by the system functionality and design. The environment and the operational rules can also influence these effects. These links are shown in Figure 3.

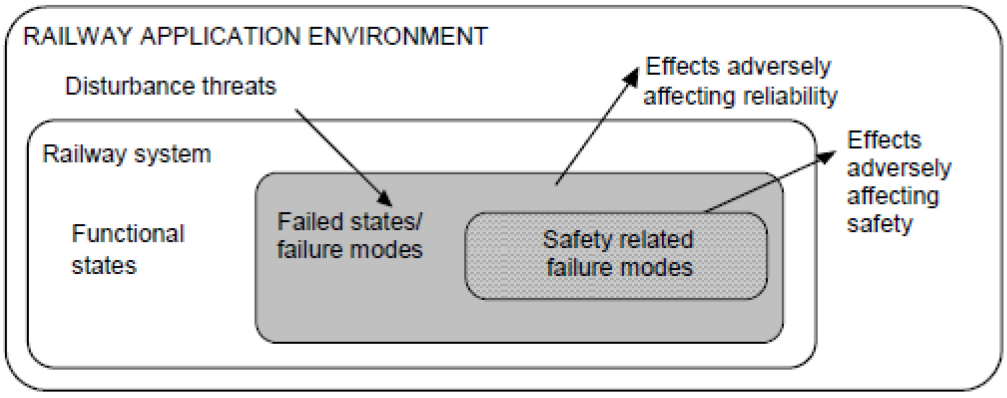


Figure 3 — Effects of failures within a system

5.6 Factors influencing railway RAMS

5.6.1 General

This subclause introduces and defines a process to support the identification of factors which influence the RAMS performance 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.

The RAMS performance of a railway system is influenced in three ways, that can interact:

- by sources of failure introduced internally within the system at any phase of the system life cycle;
- by sources of failure imposed on the system during operation; and
- by sources of failure imposed on the system during maintenance activities.

To create 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 life cycle of the system, by the application of appropriate controls to optimise system performance.

5.6.2 Classes of failures

Failures in a system, product or process are categorized as random failures or systematic failures:

- Random failures are due to causes which can be described by statistical distributions.
- Systematic failures are failures due to errors in the system life cycle activities which cause the product, system or process to fail deterministically under particular combinations of inputs or under particular conditions (e.g. combination of inputs or/and triggering events such as non-fulfilment of environmental or application conditions). Systematic failures are mainly caused by human errors in the various stages of the system life cycle. Therefore systematic failures are mainly treated by the application of appropriate processes, methods and organization.

A major distinguishing feature between random failures and systematic failures is that random failures are in general due to events that can be statistically monitored so that their probability of occurrence can be estimated. Systematic failures are due to events for which statistical data is not usually available so that their probability of occurrence cannot generally be estimated.

The clear distinction between random and systematic failures might be blurred by the following observations:

- Systematic failures are reproducible, if conditions can be exactly replicated. If these conditions (the combination of input that activates them) are by themselves a random event, the occurrence of the systematic failures also exhibit a temporal random behaviour viewed from the outside.
- Large fractions of failures, due to environmental conditions (e.g. temperature, moisture, humidity etc.) and external influences (EMC, vibration), can be considered both systematic or random as well.

Many of the normative requirements set out in Clauses 6 and 7 of this standard are aimed at the avoidance or mitigation of systematic failures.

5.6.3 Derivation of detailed railway specific influencing factors

This subclause sets out the basis of a process for the derivation of those factors which will affect the successful achievement of a system compliant with specified RAMS requirements.

Generic factors, including those contained in Figure 4, need to be reviewed in the context of the railway system under consideration.

The detailed influencing factors which influence the RAMS of a specific system shall be derived by a methodical process involving the assessment of each generic influencing factor within the context of the specific system.

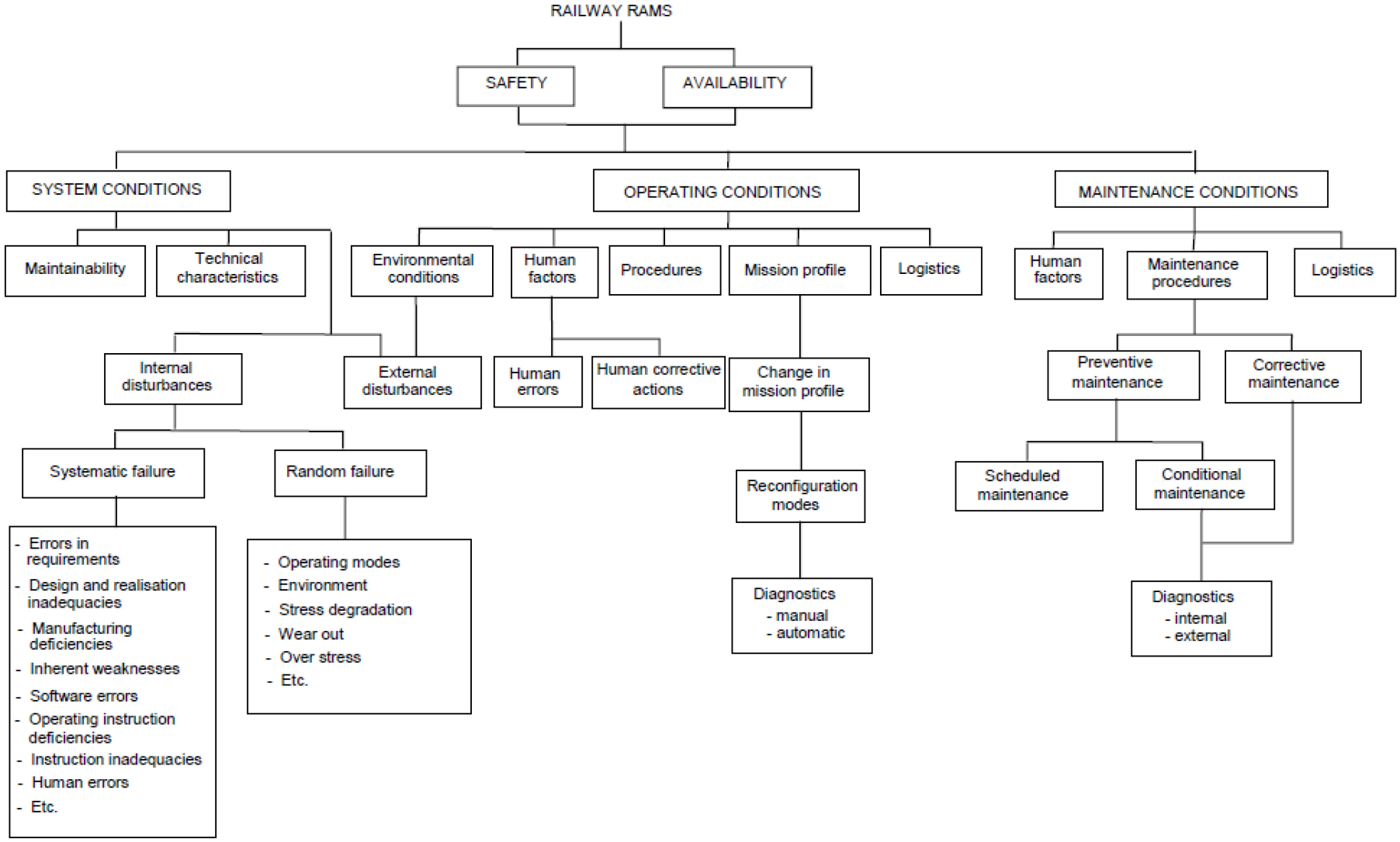


Figure 4 — Factors Influencing Railway RAMS

The process of deriving detailed influencing factors can be supported by, but not limited to, the use of the following checklist covering generic and railway specific factors. This checklist is non-exhaustive and needs to be adapted to the scope and purpose of the application.

The railway duty holder is expected to specify any applicable factors in their call for tenders.

a) system definition and system design:

- system operation:
  - the tasks which the system performs and the conditions in which the tasks will be performed (mission profile, procedures);
  - the co-existence of passengers, freight, staff and systems within the operating environment;
  - maintainability;
  - system life requirements, including system life expectancy, service intensity and life cycle cost requirements.
- failure categories:
  - the effects of failure within a distributed railway system;
  - random failure (stress degradation, wear out, overstress, etc.);
  - systematic failures (errors in requirements, design & realisation inadequacies, manufacturing deficiencies, inherent weaknesses, software errors, operating instruction deficiencies, installation inadequacies, human errors, etc.).

b) operating conditions:

- environment;
- the physical environment;
- the constraints imposed by existing infrastructure and systems on the new system under consideration;
- 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 the system on operation and maintenance;
- the need to maintain rail services during life cycle tasks (e.g. operating under degraded mode during maintenance);
- human factors;
- diagnostics;
- installation conditions;
- the integration of existing systems and new systems during commissioning and operation.

d) maintenance conditions

- preventive & corrective maintenance;
- human factors;
- logistics;
- diagnostics;
- trackside-based maintenance conditions.

It is recommended to use a diagrammatic approach to derive detailed factors, such as the use of cause/effect diagrams. An example of a much simplified cause/effect diagram is shown in Figure 5.

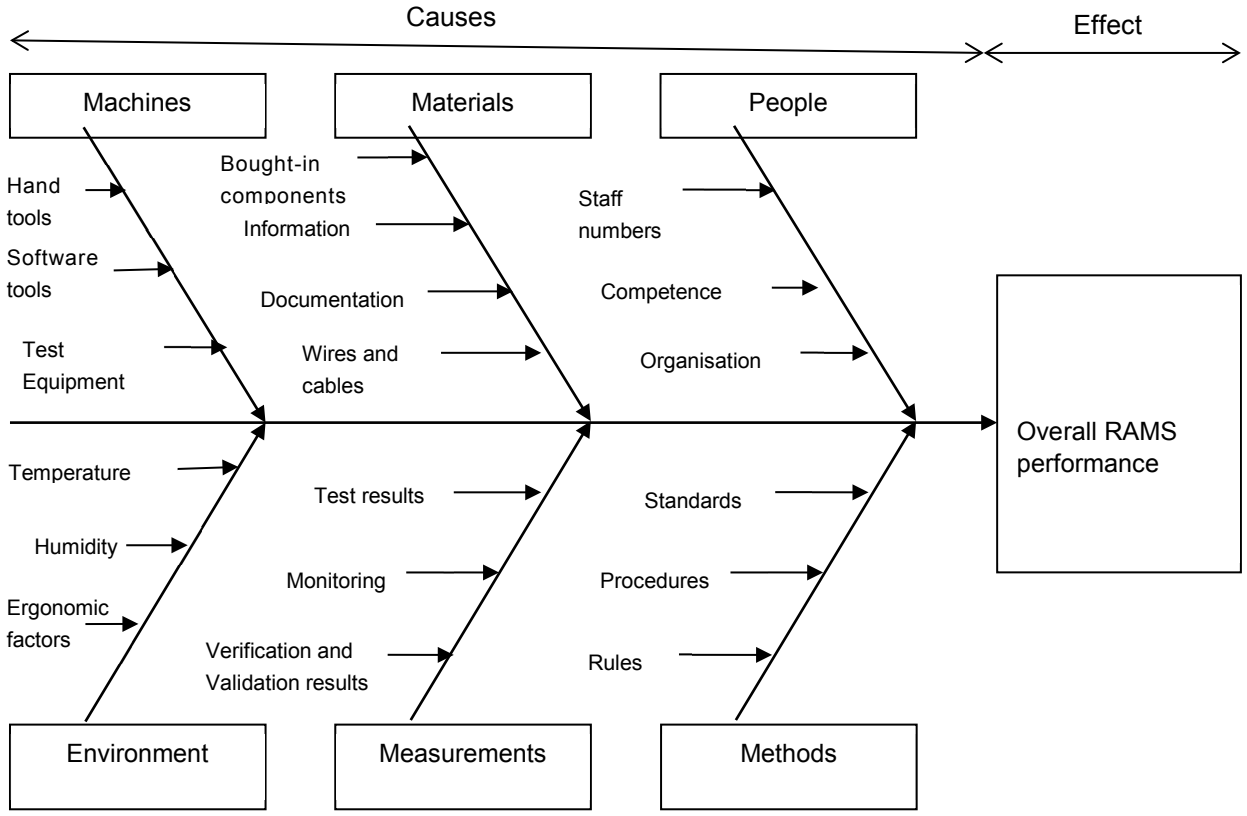


Figure 5 — Example of deriving cause/effect relations in a diagrammatic approach[2)]

In this diagram all of the elements are causes which combine to produce the effect represented by the box at the right hand side on the head of the central arrow.

- People: Anyone involved with the process
- Methods: How the process is performed and the specific requirements for doing it, such as policies, procedures, rules, regulations and laws

2) Based on “The 6 Ms” by K. Ishikawa (1960)

- Machines: Any equipment, computers, tools, etc. required to accomplish the job
- Materials: Raw materials, parts, pens, paper, etc. used to produce the final product
- Measurements: Data generated from the process that are used to evaluate its quality
- Environment: The conditions, such as location, time, temperature, and culture in which the process operates

5.6.4 Human factors

Human factors are a core aspect within an integrated RAMS management process. An analysis of human factors, with respect to their effect on system RAMS, is inherent within the “systems approach” applied by this standard.

NOTE Guidance given by standards is rare but can be found in further European Standards, such as guidance on ergonomic design in EN 614.

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.

Each human might react to situations in different ways, which impacts the RAMS performance. The achievement of railway RAMS requires more rigorous control of human factors, throughout the entire system life cycle, than is required in many other industrial applications.

Humans have the ability to influence the RAMS of a railway system positively or negatively. To maximise the positive influence and minimise the negative influence, the manner in which human factors can influence railway RAMS shall be identified and managed throughout the life cycle. This shall include the potential impact of human factors on railway RAMS not only within the Operation, Maintenance and Performance Monitoring phase, but also within the other phases of the system life cycle. The precise influence of human factors on RAMS is specific to the application under consideration.

Specific standards for guidance and methods to analyse the influence of human factors on RAMS can be considered.

EXAMPLE: Example of standard is VDI 4006 “Human Reliability”.

Human influence can be regarded as having both random and systematic aspects. All humans are subject to occasional lapses in performance. When these occur in the operational and maintenance phases of the system life cycle they tend to result in random failures: when they occur in earlier phases of the life cycle they can result in systematic failures in the operational phase.

Lack of competence can lead to systematic human error, where lack of knowledge or understanding can result in the same incorrect action always being taken under the same circumstances. This can affect all phases of the life cycle.

The derivation of detailed human influencing factors can be supported by, but not be limited to, a consideration of each of the following human factors. The following checklist is non-exhaustive and needs to 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 organisational 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 for 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 provision of user manuals etc.;

– the effect of human error;

– the effect of deliberate human rule violation (e.g. where an operator ignores a rule in order to save time);

– 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;

– human reaction under different operating modes (e.g. normal, degraded or emergency).

f) human factors in all phases of the system lifecycle, including:

– human competency;

– human independence during design, verification and validation;

– human involvement in verification and validation;

– interface between human and automated tools;

– systematic failure prevention processes (e.g. measures to assure safety integrity).

5.7 Specification of railway RAMS requirements

5.7.1 General

The main goal of RAMS activities is to achieve a system performance that meets the RAMS requirements. Therefore, specification of proper RAMS requirements is of utmost importance. Additional information on methods for deriving and specifying system safety requirements is set out in EN 50126-2.

To achieve the required RAMS requirements, the parameters influencing the RAMS performance shall be controlled throughout the life cycle of the system. Effective control requires the establishment of mechanisms and procedures which are defined in Clauses 6 and 7 to defend against sources of failure. Such defences need to take account of both random and systematic failures.

5.7.2 RAMS specification

The specification of RAMS requirements is a complex process.

Examples of typical parameters to characterise reliability, availability, maintainability, logistic support and safety requirements for railway systems are shown in Annex B. Specific parameters will depend on the system under consideration. All relevant RAMS parameters shall be agreed between the railway duty holder and the railway supplier on the basis of the rules given by the legal framework. Where parameters can be expressed in alternative dimensions, conversion factors shall be provided.

A list of suitable tools for RAMS activities is also included in A.4. 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.

5.8 Risk based approach

The risk based approach involves managing RAMS activities based on decisions which are derived from considerations of risk. It aims to identify risks, derive requirements and implement measures to avoid or control these risks. This approach is fundamental to the RAMS management process and allows RAMS risk to be managed through the whole product life cycle.

The risk based approach is characterised by judgement against risk acceptance criteria of the acceptability of the residual risks remaining after the implementation of control measures. The risk evaluation and acceptance criteria to be applied shall be defined on the basis of the system definition (7.3).

Defining the correct risk evaluation and acceptance criteria for safety risks is of critical importance because they can concern low frequency and high consequence events with the potential to harm people. Detailed requirements for safety risk evaluation and acceptance criteria are given in 6.3 and 7.4.

Although the term risk is more commonly associated with safety than with RAM, it is applicable to all aspects of RAMS. Risk is the combination of two elements, each one applicable to safety and to RAM:

- the expected frequency of occurrence of loss; and
- the degree of severity of this loss (consequence).

When performing RAM activities, risk definition can be completed by adding the ability to detect the failures impacting reliability.

Loss can imply human, property, and/or environmental harm. Informative details are provided in Annex C.

Environmental loss is often taken into account in a qualitative manner, and usually not included in the safety studies. However, it is recommended that its exclusion is agreed between the railway stakeholders including the relevant safety authority, as long as there are no contradictions to the given legal framework.

5.9 Risk reduction strategy

5.9.1 Introduction

The strategy of risk reduction applies to all risks related to RAMS. The objective of the strategy is to reduce risk to an acceptable level whenever a risk is analysed as being not acceptable.

The risk can be decreased by taking a combination of precautions to reduce the loss by decreasing the frequency of events which result in loss, and to mitigate the loss by reducing its severity. Prevention is generally considered to be preferable to mitigation in most circumstances.

As an additional perspective to the application of the RAMS management process, the following guidance derived from ISO/IEC Guide 51 is given. It concentrates on risks related to safety. Nevertheless, these considerations can be applied to RAM as well in an adapted sense.

5.9.2 Reduction of risks related to safety

This subclause describes a best practice approach to reduce safety risk in which the following steps are applied in sequence and assessed on the basis of their practicability.

An initial goal of any safety-related activity is to determine if the hazard can be practicably avoided. If this is not possible, the next consideration is whether the frequency of occurrence of the hazard could be reduced to an acceptable level.

If not sufficient, the next goal is to ensure that the frequency of a hazard turning into an accident is kept as low as possible.

If this cannot be reduced sufficiently, the final step is to minimise the severity of loss, resulting from the accident (hazard's consequence).

The approach and the steps necessary to ensure safety in designing equipment as well as for setting operational rules are:

a) make the function under consideration safe.

   The safe failure mode is a relative concept, and the related arguments are provided when performing analysis. Some systems do not have one single status that is safe under all circumstances.

   EXAMPLE: Automatically stopping a train if an emergency is detected is usually safe but sometimes dangerous (e.g. burning train stopped in a tunnel).

b) If necessary, provide additional safety functions or some other barriers.

   Functions dedicated to increasing safety are implemented wherever necessary to satisfy the relevant risk acceptance criteria. This applies for all technologies and for operational rules as well. The

performance of these safety functions needs to be adequately checked at sufficiently frequent intervals.

c) If necessary, provide safety-related information in addition.

According to the above, additional measures will be necessary, expressed as additional constraints improving safety (e.g. related to application, maintenance or operation).

More requirements and supporting guidance for safety aspects can be found in EN 50126-2.

5.9.3 Reduction of risks related to RAM

The reduction of RAM risk is concerned with reducing loss to the value of the service provided by the railway (e.g. train delays or cancellations). This subclause outlines the ways in which activities at each phase of the system lifecycle can contribute to the reduction of RAM risk.

The principal ways in which RAM risk can be reduced are:

- improvement in reliability, so that fewer failures occur with consequently fewer occasions for loss;
- improvement in availability, so that when a failure does occur the resulting loss is smaller.

Measures to improve reliability with regard to random failures include:

- designing system tolerances so that small deviations of parameters from their nominal values do not result in incorrect operation (phase 6, Design and Implementation)
- designing so that components are not expected to operate close to their limits e.g. rated load, temperature, etc. (phase 6, Design and Implementation)
- application of good quality management practices to the procurement of materials and to the control of manufacturing and installation processes (phase 7, Manufacture)
- condition monitoring and preventive maintenance (phase 11, Operation, Maintenance and Performance Monitoring)

There are four principal strategies for improving availability:

- provision of duplicate or back-up systems so that a single failure does not result in any loss of function (phase 5, Architecture and apportionment of system requirements).
- provision of facilities for operation in a degraded mode (e.g. reduced train frequency or reduce speeds) in the event of a failure (phase 2, System definition and operational context, and phase 5, Architecture and apportionment of system requirements)
- improving the maintainability of the system, so that the time required for repair and restoration of normal operation following a failure is reduced (phase 6, Design and Implementation)
- provision of sufficient resources (such as competent staff, test equipment, spares) so that the time required for repair and restoration of normal operation following a failure is reduced (phase 11, Operation, Maintenance and Performance Monitoring)

These strategies can be applied in combination. The order in which they are listed does not imply an order of preference.

Systematic failures are also a significant source of RAM risk and the activities at every phase of the lifecycle aimed at preventing systematic failure, such as specification, verification and validation, contribute to the reduction of RAM risk by giving appropriate attention to RAM aspects.

Consideration of RAM in phases 1 to 4 of the system lifecycle enables an appropriate combination of measures and strategies to be adopted.

6 Management of railway RAMS – general requirements

6.1 Introduction

This clause provides general requirements for management of railway RAMS.

The life cycle model for the system under consideration is defined as a basis for the management of RAMS, including adaptability rules.

Detailed requirements related to life cycle phases are provided in Clause 7.

Specific requirements for Safety activities are provided in EN 50126-2.

6.2 Life cycle for the system under consideration

The life cycle approach provides a structure for planning, managing, controlling and monitoring all aspects of a system, including RAMS, as the system under consideration progresses through the life cycle phases.

The focus of the RAMS process is to reduce the incidence of failures and/or the consequences throughout the life cycle, and thus minimise the residual risk resulting from these errors.

The life cycle model is fundamental to the successful implementation of this standard. The reference model is described in Figure 6.

This standard represents the life cycle sequentially. This representation shows individual phases and the links between phases. Other life cycle representations are widespread within industry and may be used as long as they follow the requirements of this standard.

The general RAMS process consists of 3 major blocks:

- Risk assessment (on the basis of the system definition), including the specification of RAMS requirements,
- Implementation and demonstration that the system fulfils the specified RAMS requirements, and
- Operation, maintenance and decommissioning.

Besides the nominal process flow between the life cycle phases, the general process includes:

a) a feedback loop (on the right side of Figure 6):

– new or additional knowledge about risk come up during any phase of the project requiring the risk to be reassessed;

b) subsequent loops for control of RAMS requirements (on the left side of Figure 6):

– reassessment allowing to skip some phases of the regular process flow if the reconsidered RAMS requirements do not affect those phases; or

– in worst case, reassessment demanding rephrasing of the remit of the project (concept phase) if the requirements cannot be met in any way.

A direct consequence of these loops is that the logical flow of information and decision is more important than the time based flow of the phases. Therefore, generally the risk assessment needs to be confirmed also at the end of the life cycle.

The general project tasks are outside the scope of this European Standard. RAMS tasks contribute to the general project tasks for each life cycle phase, and requirements for the RAMS tasks are detailed in subsequent clauses of this European Standard.

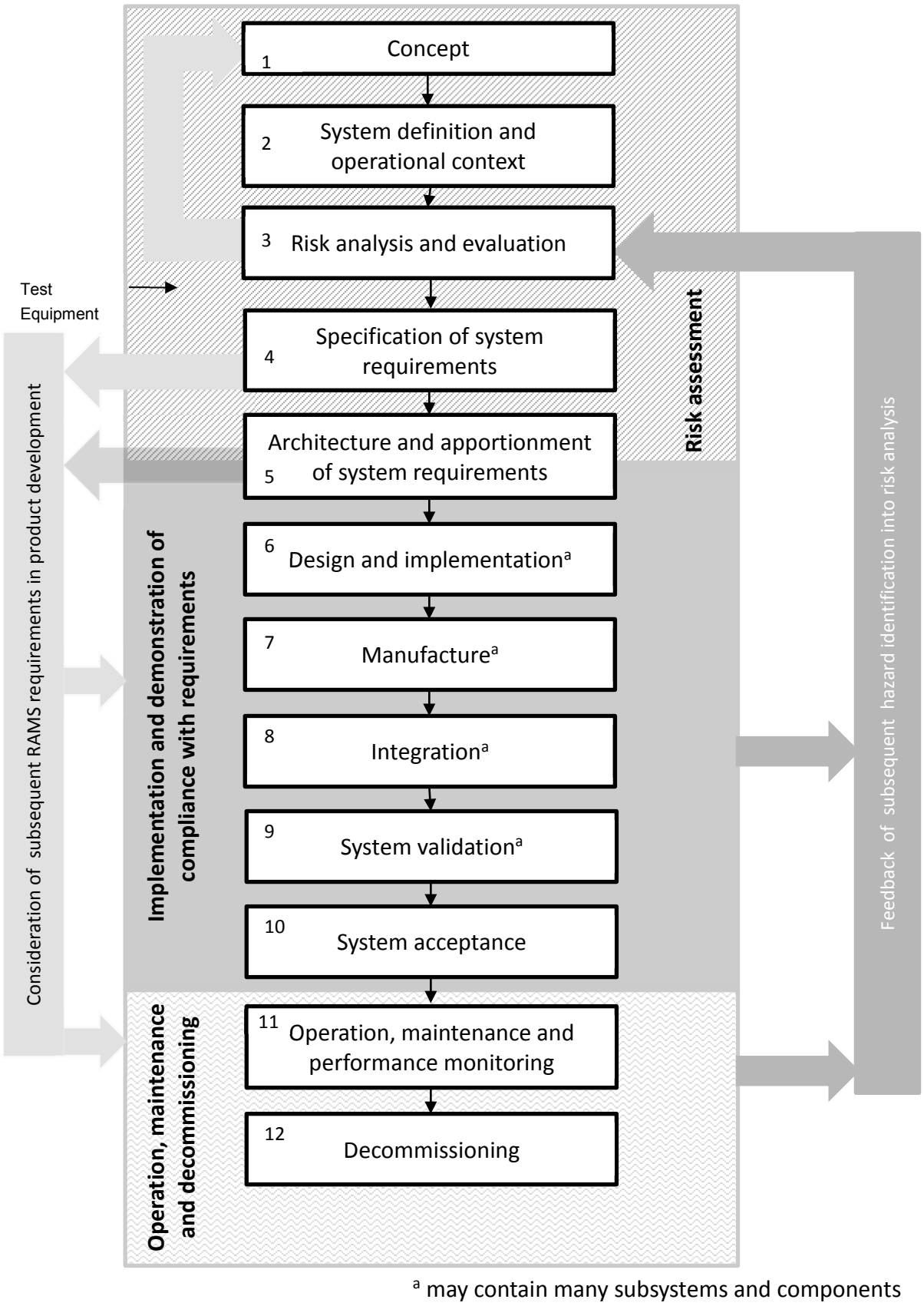


Figure 6 — Interrelation of RAMS management process and system life cycle

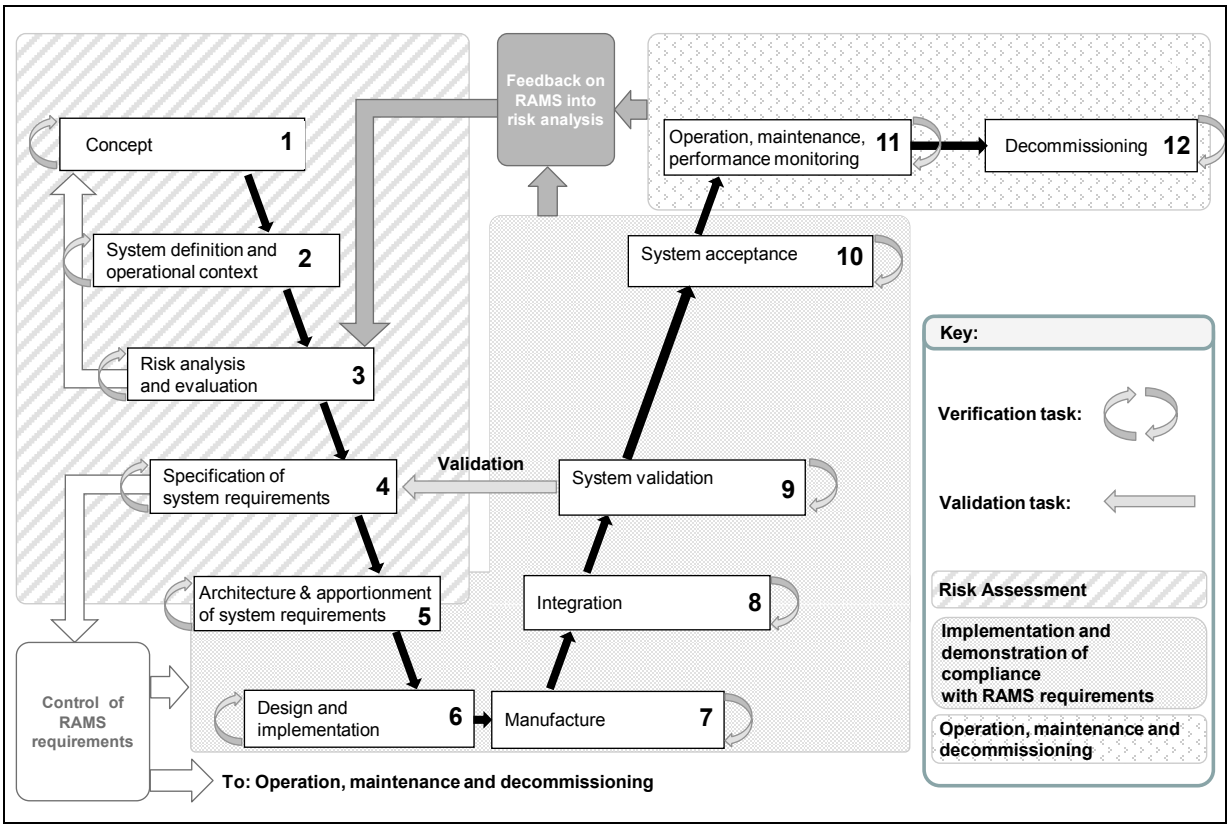


Figure 7 — The V-cycle representation

NOTE 1 The proposed life cycle in Figure 7 has a "V" representation. 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 hand-over and then the operation and maintenance of the whole system.

NOTE 2 Verification and Validation tasks are defined in 6.7.

Life cycle phases are:

1. Concept (see details in 7.2): remit of the project should be drawn up;

2. System definition and operational context (see details in 7.3): description of essential characteristics and functions of the system, and clarification of the interfaces to other systems including the input to be provided and the output that can be expected. On this basis the impact on RAMS parameters of neighbouring systems can be derived. The intended operational conditions (maintenance, environment, etc.) that could impair the safe or good (RAM) function are stated to ensure that the operator is aware of them. The RAMS management is established, including RAM plan and Safety plan;

3. Risk analysis and evaluation (see details in 7.4): several steps (e.g. for safety: identify hazards associated with the system, identify events leading to hazards, determine risk associated with hazards, establish process for on-going risk management) should be followed to decide if a risk is tolerable. Risk analysis is an ongoing and iterative step and can continue in parallel with subsequent phases. It can be necessary to define further system safety requirements induced by the Risk Acceptance Criteria in order to reduce the risk to an acceptable level. System requirements can be derived / exist at different levels;

4. Specification of system requirements (see details in 7.5): detailing the initial system requirements (expected functions including their RAMS requirements) and the ones derived from risk assessment

in phase 3 as well as defining criteria for acceptance and specifying the overall demonstration of compliance;

5. Architecture and apportionment of system requirements (see details in 7.6): allocation of requirements (including all RAMS requirements) to subsystems;

NOTE 3 Subsystem requirements can be directly allocated if they are already available at this level or are apportioned by deriving them from system level requirements.

6. Design and implementation (see details in 7.7): subsystems and components should be created according to the allocated requirements (including RAMS requirements);

7. Manufacture (see details in 7.8): the subsystems and components of the system should be manufactured and RAMS centred assurance arrangements established and applied;

8. Integration (see details in 7.9): all subsystems and components should be assembled and installed to form the complete system;

9. System validation (see details in 7.10): it should be validated that the system, product or process complies with the RAMS requirements in combination with external risk reduction measures, confirming that it is suitable for a specific intended use;

10. System acceptance (see details in 7.11): compliance of complete system with overall RAMS requirements is required for entry into service;

11. Operation, maintenance and performance monitoring (see details in 7.12): The objective of this phase is to operate, maintain and support the product, system or process such that compliance with system RAMS requirements is maintained. This includes to continuously evaluate the RAMS performance of the system and to derive corrective measures if required;

12. Decommissioning (see details in 7.13): the risk is controlled during the transition phase.

In case of subordinated system level, sub-clause 6.5 defines which phases need to be repeated. Principally this relates to all life cycle phases. Each subsystem should be addressed in the same manner at their level of detail and within the boundary of their specific subsystem definition (iterative method).

When information about hazards and associated risks in later phases of the life cycle conveys additional hazards or a higher risk than assumed earlier in the life cycle, the prolonging validity of the initial risk assessment shall be shown again or an update of the initial risk assessment shall be provided.

Whenever changes are introduced after completion of the acceptance phase, the risk assessment phase of the life cycle shall be reapplied, including evaluation of the impact on subsequent life cycle phases.

NOTE 4 Changes introduced during “Implementation and demonstration of compliance with RAMS requirements” block of the RAMS life cycle, could be managed based on a change control management process (e.g.: bug resolution).

Table 1 summarizes, for information, the relationship between RAMS tasks to be considered throughout the lifecycle of the system under consideration. Requirements for each life-cycle phase are detailed in Clause 7.

Table 1 (informative) — RAMS tasks for lifecycle phases 1 to 12

Phase	*Phase*	*Clause*	*General tasks*	*RAM tasks*	*Safety tasks*
1	Concept	7.2	Investigate scope, context and purpose of the system. Investigate the environment of the system.	Investigate the general RAM implications of the system. Investigate previous RAM requirements and past RAM performance of similiar/related systems. Investigate current RAM policy and targets of the relevant railway duty holders. Define the scope of the RAM management requirements for subsequent system life cycle RAM tasks.	Investigate the general safety implications of the system. Investigate previous safety requirements and past safety performance of similiar/related systems. Investigate current safety policy and targets of the relevant railway duty holders. Investigate safety legislation. Define the scope of the safety management requirements for subsequent system life cycle safety tasks.
2	System definition and operational context	7.3	Define the system and its mission profile. Define the system boundary. Define the scope of operational requirements. Establish the organisation.	Establish the RAM policy. Establish the RAM plan.	Establish the safety policy. Establish the safety plan.
3	Risk analysis and evaluation	7.4		Perform Risk Analysis. Update RAM Plan.	Perform risk analysis. Establish hazard log. Update Safety Plan. Establish Independent Safety Assessment Plan.

Phase	*Phase*	*Clause*	*General tasks*	*RAM tasks*	*Safety tasks*
4	Specification of system requirements	7.5	Specify system requirements	Establish RAM requirements specification. Update the RAM plan. Establish validation plan for RAM requirements.	Establish safety requirements specification. Establish safety-related application conditions. Update hazard log. Update the safety plan. Establish validation plan for safety requirements.
5	Architecture and apportionment of system requirements	7.6	Define the system architecture. Identify the requirements for integration of pre-existing subsystems/components. Define acceptance criteria and processes for subsystems/components.	Allocate RAM requirements to subsystems/components. Update the RAM plan. Update validation plan for RAM requirements.	Perform hazard analysis. Allocate safety requirements to subsystems/components. Update safety-related application conditions. Update hazard log. Update the safety plan. Update validation plan for safety requirements.
6	Design and implementation	7.7	Design subsystems/components. Prepare operation and maintenance procedures. Define training measures for operation and maintenance. Define and establish manufacturing process for producing subsystems and components. Define and establish system integration process. Prepare installation and commissioning procedures.	Plan RAM tasks of further phases. Perform RAM analysis. Update the RAM plan. Update validation plan for RAM requirements.	Plan safety tasks of further phases. Perform hazard analysis. Update safety-related application conditions. Update hazard log. Update the safety plan. Update validation plan for safety requirements. Prepare safety case.

Phase	*Phase*	*Clause*	*General tasks*	*RAM tasks*	*Safety tasks*
7	Manufacture	7.8	Implement and operate manufacturing process.	Establish RAM assurance arrangements. Update the RAM plan. Update validation plan for RAM requirements.	Establish safety assurance arrangements. Update safety-related application conditions. Update hazard log. Update the safety plan. Update validation plan for safety requirements. Update safety case.
8	Integration	7.9	Integrate subsystems and components. Demonstrate system functionality. Test and analyse system. Arrange system support arrangements.	Establish integration report for RAM requirements. Update the RAM plan. Update validation plan for RAM requirements.	Establish integration report for safety requirements. Update safety-related application conditions. Update hazard log. Update the safety plan. Update validation plan for safety requirements. Update safety case.
9	System Validation	7.10	Establish validation report. Establish process for the acquisition and evaluation of operational and maintenance data.	Establish RAM validation report.	Esatblish safety validation report. Update safety-related application conditions. Update hazard log. Update the safety plan. Update validation plan for safety requirements. Update safety case.
10	System acceptance	7.11	Record an acceptance record. Verify the acceptance record.	Assess RAM validation.	Establish Independent Safety Assessment Report. Assure endorsement of safety-related application conditions.

Phase	*Phase*	*Clause*	*General tasks*	*RAM tasks*	*Safety tasks*
11	Operation, maintenance and performance monitoring	7.12	Provide all information necessary to formulate plans/procedures for operation and maintenance. Implement operation and maintenance procedures. Record changes in the system configuration.	Implement and maintain FRACAS process for the acquisition and recording of RAM performance data. Maintain FRACAS and periodically review FRACAS records. Establish records to trace the RAM tasks undertaken. Reports of RAM performance analysis and evaluation.	Implement and maintain process for the acquisition and recording of safety performance data. Perform an impact analysis in case of changes and reapply process if needed. Records to trace the safety tasks undertaken. Establish reports of safety performance analysis and evaluation.
12	Decommissioning	7.13	Establish decommissioning plan and related report.	Identify the RAM impact of decommissioning and disposal.	Identify the safety impact of decommissioning and disposal.

NOTE Change Control or Configuration Management activity applies to all project phases.

6.3 Risk assessment

This chapter is relevant for life cycle phase 3 and based on the system definition of life cycle phase 2. It can be necessary to evaluate the risk assessment in life cycle phase 10 and/or 11. It can also be continued as appropriate at various phases of the system life cycle.

The risk assessment process is shown in Figure 8. It comprises both:

- Risk analysis;
- Risk evaluation.

Risk analysis is the systematic use of all available information to identify hazards or its RAM equivalent, related potential losses and to evaluate the associated risk.

Risk analysis distinguishes between the hazards or its RAM equivalents that do not need to be analysed further, from the hazards or RAM equivalents that need to be further analysed.

The following text is applicable in the case of losses related to hazards and may be applied also to RAM equivalents.

NOTE 1 RAM equivalent to hazard is a condition that could lead to commercial loss related to RAM.

A risk assessment shall be undertaken for the system under consideration. For each identified hazard or its RAM equivalent, it shall be decided if the related risk can be considered as “broadly acceptable”. This decision shall be justified and recorded. As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional measure. The expert judgement shall take into account that the contribution of all the broadly acceptable risks does not exceed a defined proportion of the overall risk.

NOTE 2 The choice of “broadly acceptable risk” can include cases where no injury to humans apply or cases with no consequences on safety but only on availability. In these cases requirements for RAM can still apply.

If the risk analysis identified cases with risk "broadly acceptable", there is no need to specify further requirements for those cases.

If the risk analysis concluded that a risk is not "broadly acceptable”, the risk analysis activity shall be continued by choosing and applying a ‘risk acceptance principle’ (RAP), before applying risk evaluation. The three risk acceptance principles are:

a) use of Code of Practice (CoP);

b) comparison with a similar system as a reference;

c) Explicit risk estimation (ERE) (qualitative or quantitative).

Once the RAP has been chosen and applied, the process continues with the risk evaluation (determing the achievement of the criteria associated to the selected RAP) and the specification of safety requirements.

The tolerable safety risk of a railway system is dependent upon the risk acceptance criteria (RAC) set by the legal framework, or by the railway duty holder in accordance with the rules given by legal framework.

NOTE 3 Details for safety, including specification of basic integrity and safety integrity, is provided in EN 50126-2.

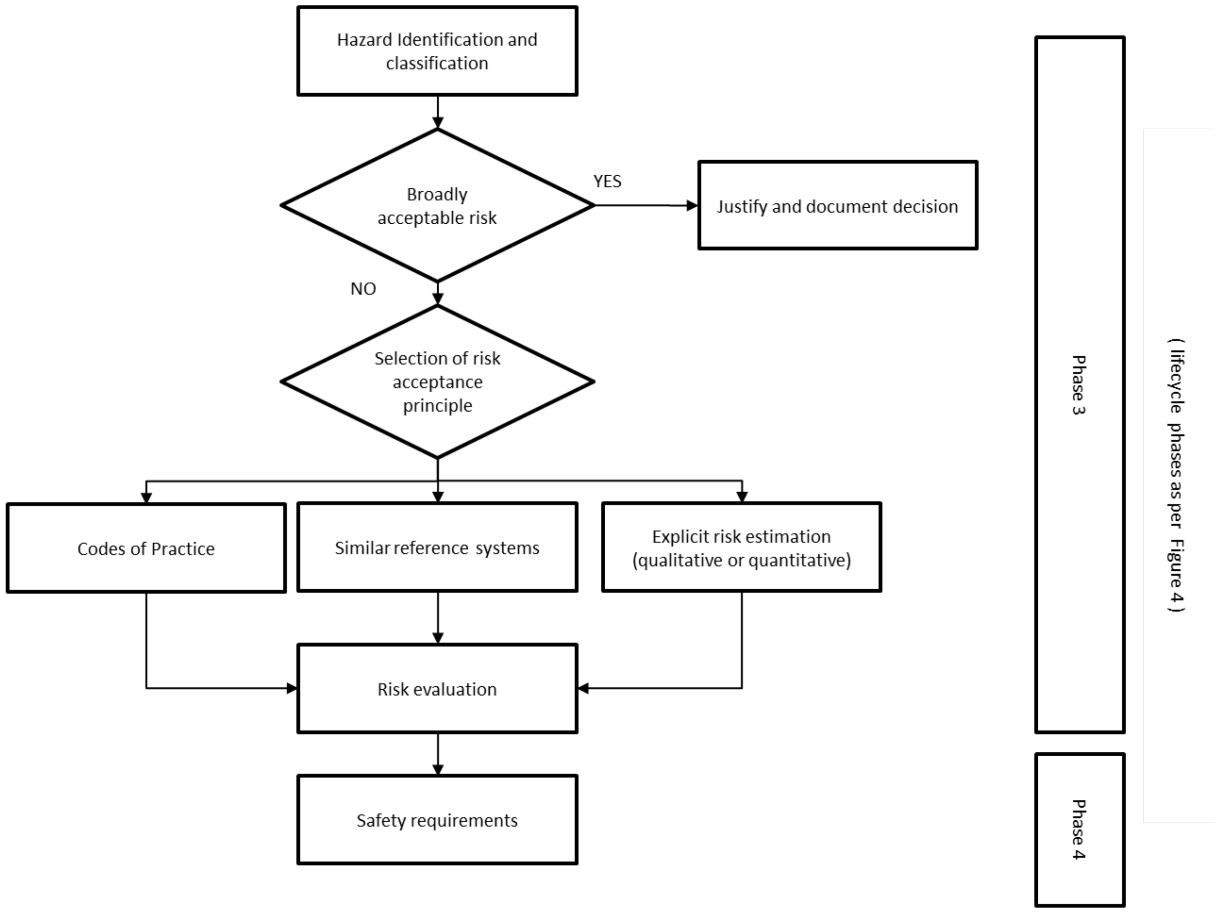


Figure 8 — Process for Risk Assessment related to phases 3 and 4 (as per safety)

6.4 Organisational requirements

6.4.1 Introduction

Fulfillment of the requirements of this standard relies on organisational structures and rules, embodied by the management in charge, that enable their staff to comply with the more detailed requirements and ensures that they are being followed. Therefore this standard assumes management commitment and action.

The responsibilities for the tasks in the various life cycle phases depend on the contractual and legal relationship between the parties involved, with related roles and responsibilities defined and agreed.

In the context of a procurement process, roles and responsibilities for carrying out RAMS tasks should be clarified. Responsibilities for carrying out the tasks will depend on the system under consideration and the contract conditions applicable.

Many roles within an organisation, such as verifier, validator or assessor, are concerned with confirming the RAMS performance of what has been produced by other roles (e.g. designer).

Independence between roles can be required in order to reduce the probability of people in different roles suffering from the same misconceptions or making the same mistakes. This form of independence can be achieved by employing different people in different roles but does not usually require the roles to be located in different parts of the organisation or in different companies.

It is also important that people in roles which involve making judgements about the acceptability of a product or process from the point of view of safety should not be influenced by pressure from their peers or supervisors, or by considerations of commercial gain.

In general, a greater degree of safety risk requires a greater degree of independence for various roles.

A given role (e.g. designer, verifier, validator, assessor) can be assigned to a different stakeholder for each of the three main blocks of the life cycle (Risk assessment, Implementation and Demonstration of Compliance, Operation and Maintenance) defined in 6.1.

Verification and Validation of the Risk assessment is generally a different task from Verification and Validation of the Implementation and Demonstration of Compliance, and can be ruled by different contractual requirements with different sets of documentation.

6.4.2 Requirements

The RAMS management process shall be implemented under the control of an appropriate organisation, using competent personnel assigned to specific roles.

Assessment and documentation of personnel competence, including technical knowledge, qualifications, relevant experience and appropriate training, shall be carried out in accordance with documented requirements to be defined by the RAMS management organisation.

The level of technical education, the extent of experience, and the need for updating or refreshing of training shall be commensurate to the RAMS requirements for the application.

Roles and Responsibilities for the tasks in the various life cycle phases shall be defined.

Rules for independence between roles shall be defined. Minimum requirements for safety are defined in EN 50126-2:2017, Clause 7.

Within the limits given by requirements on the independence of roles, one person may carry out more than one role.

6.5 Application of this standard and adaptability to project scope and size

6.5.1 General requirements

This subclause provides requirements for a flexible and effective application of this standard in terms of size and complexity.

The RAMS management process described in this standard is based on the lifecycle model applied to the system under consideration. The extent of the application of the requirements defined in Clause 7 to the system under consideration shall be defined in the RAMS Plan.

A life cycle model for the development of the system under consideration shall be selected. The life cycle model shall take into account the possibility of iterations in and between phases.

The following requirements shall remain normative:

- responsibilities for carrying out RAMS tasks including the interfaces between associated tasks shall be defined for the system under consideration;

- all personnel with responsibilities within the RAMS management process shall be competent for those responsibilities;

- RAM Plan and Safety Plan shall be established;

The quality management system should conform to EN ISO 9001 rules or equivalent rules and be appropriate for the system under consideration;

NOTE Conformity to these requirements is sufficient for the quality management of the RAM requirements and is a necessary basis for the safety management which is needed to fulfil the safety requirements;

- an adequate configuration management system, addressing RAMS tasks, shall be used. The scope of configuration management will depend on the system under consideration, but shall at least include system documentation.

The application of this standard may be tailored allowing requirements of Clause 7 to be scaled to the specific requirements for the system under consideration. This tailoring should consider the following aspects:

- constraints given by the railway duty holder;
- complexity of the system under consideration;
- the application domain (i.e. signalling, rolling stock, fixed installations);
- the system development process used;
- type of development (e.g. generic product, specific application, modification of existing system).

The process may be simplified by reusing existing applicable material.

EXAMPLE An example of such material which can be reused in this way is the Technical Specification CLC/TS 50562:2011, “Railway applications - Fixed installations - Process, measures and demonstration of safety for electric traction systems”.

All requirements within the standard which the applicant of the standard decides to scale or omit for tailoring purposes shall be explicitly identified.

NOTE The entity applying the standards is responsible for applying the requirements to each life cycle phase for which they are responsible. Responsibility for compliance can arise for a number of reasons such as, contractual obligation, legal obligation, or where the standard user wishes to claim compliance with the standard. Evidence of the tailoring proposed by the user of the standard enables the explicit agreement of these aspects to be reached between the purchaser and user.

In case of tailoring, the following specifications and justifications shall be elaborated:

a) specify the life cycle phases which are required to realise the system under consideration and demonstrate that the tasks undertaken within these life cycle phases comply with the principles of the requirements of this standard;

b) specify the life cycle phases which are not required to realise the system under consideration and provide an appropriate justification;

c) specify the activities and requirements of each required life cycle phase, using Table 1 and the relevant phase related information of Clause 7, 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;

d) justify the limit of applicability for tasks and requirements of the standard.

In practical applications, the system under consideration can be:

- part of a wider system and/or incorporate narrower systems (subsystems, products, …) managed with their own RAMS process (see 6.5.2);
- part of a renewal scope, including or interfacing existing systems, with possible “mixed phase” stage (see 6.5.3);

- a re-use or adaptation of a system already accepted, including specific application of a defined Generic Product / Application (see 6.5.4).

Where a system includes an element of COTS subsystems or equipment there can also be a need to tailor the process as described in this standard.

6.5.2 Case of complex systems with different hierarchical levels

When defining the lifecycle of a given system under consideration, it shall be defined which subordinated systems (subsystems / products) will be incorporated and, as far as known, which superior system has originated requirements.

The definition of the related application scope will allow the lifecycle identifying which phases will be completely or partially addressed by the RAMS management process.

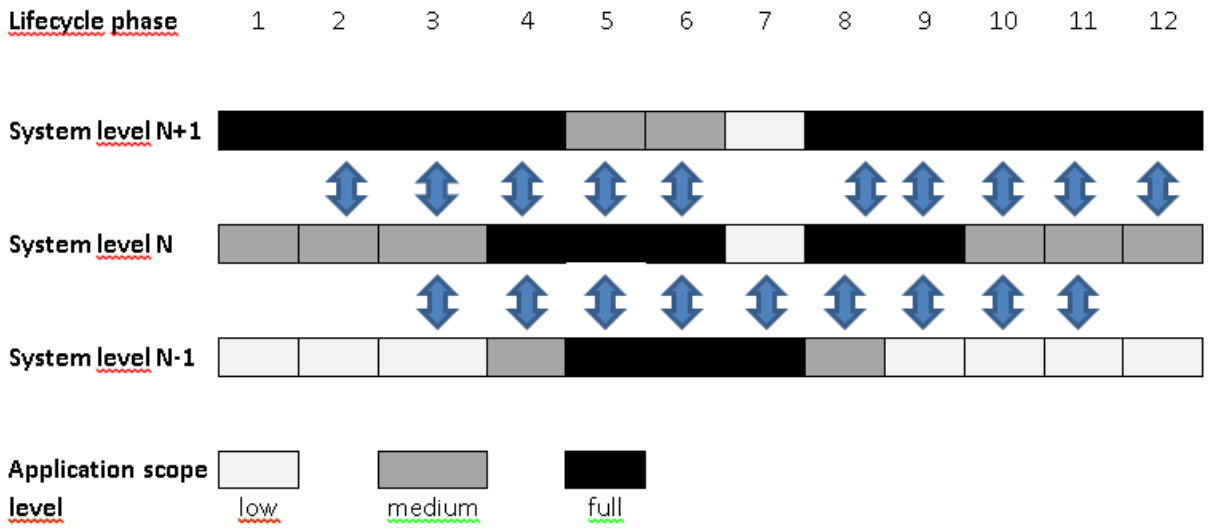


Figure 9 — Example of lifecycles at different hierarchical levels

NOTE 1 The Figure shows the relationship between Level N, that is the system under consideration for which the entity applying the standard is responsible, with the superior system level N+1 and the subordinate system level N-1. The entity applying the standard for the system under consideration is responsible for the integration of the subordinate systems. The responsibility for the integration of the system under consideration into a superior system is of the related entity.

NOTE 2 The degree of shading in the figure varies from darkest colour (intended as tasks of the related phase expected to be completely applied), to lightest colour (intended as tasks of the related phase expected to be partially applied).

Whenever the scope of a lifecycle phase for a system at level N can impact the RAMS management process of the system at level N+1 or level N-1, level N shall describe the relationship between the related safety management processes if known, and if not known clearly identify the related assumptions and record the related constraints in application conditions.

EXAMPLE In Figure 9, phases 1 to 4 for a subordinated system are of lighter colour because a requirements specification and list of applicable hazards for a constituent can be defined regardless the preventive definition of a system at superior level. Once the assumptions are clearly defined and documented, it will then be the superior system that will assure relationships between its requirements and applicable hazards with the ones of the incorporated constituent.

RAMS assumptions on boundary interfaces shall be explicitly stated and referenced during the life cycle phase of system definition.

RAMS constraints related to the introduced interfaces in case of incorporation of new or existing systems (subsystems, products, etc.) shall be explicitly defined and referenced during phase 5 (Architecture and apportionment of system requirements).

The RAMS management process shall specify how application conditions related to RAMS are managed and communicated to relevant stakeholders for fulfilment. This includes:

– application conditions exported from incorporated subordinated systems (subsystems, products, etc.) during the phase of integration;

– application conditions exported to superior system and other stakeholders.

6.5.3 Renewal within existing systems

The RAMS management process shall consider the possible effects of interaction between the existing and renewed systems, including assumptions on safety performances of existing systems.

NOTE In case of changes involving systems already accepted, the impact on the RAMS of neighbouring systems via interfaces and the resulting impact on RAMS of the railway system operation need to be investigated. The system definition determines the outline of assessment with the description of boundaries and interfaces and since the process itself is scalable to system, subsystem or product level, the extent and depth of the analysis can be adjusted to an appropriate level for the task at hand.

During the risk assessment the possible hazards / RAM equivalents resulting out of the change are identified (interfaces included), evaluated and the resulting requirements are defined and possibly apportioned. After that, only the affected phases of the process will be reconsidered.

If the change does not create additional risk (e.g. by creating a new hazard or a RAM equivalent, making an existing hazard or RAM equivalent more likely or changing the consequences of a hazard or its RAM equivalent), the related argument will be documented.

The same requirements applies to the cases of renewal of a system, whenever a "mixed phase" stage where the operation with the existing and the renewed systems is mixed, or when they are operated at the same time.

6.5.4 Re-use or adaptation of a system with previous acceptance

In case of re-use or adaptation of a system with previous acceptance, a mutual recognition (sometimes referred to as cross acceptance) of previous acceptance may be applied limiting the effort on the related lifecycle. This case is considered as a special case of tailoring.

NOTE 1 Legal aspects implied by these topics are out of the scope of this standard and need to be dealt with considering the legal framework.

NOTE 2 The tailoring discussed in this sub-clause has the purpose to reuse existing results and documents compliant with this standard that have been created in other developments and avoid repetition of processes/tasks.

This case may also be applied to specific application of a defined generic product / application as defined in Clause 8.

In case of re-use or adaptation of a system with previous acceptance, the following principles should be addressed:

a) establish a credible argumentation with evidences for the original reference application;

b) specify the target environment and application;

c) identify the differences between the modified and original reference application, including evidence that the operational and environmental context of the new application is identical/similar to the original one and the process-related and technical requirements are still appropriate in the new application;

d) specify the technical, operational and procedural adaptations required to cater for the differences;

e) assess the risks arising from the differences;

f) produce a credible argumentation with evidences for the adaptations adequately controlling the risks arising from the differences;

g) develop a generic or specific argumentation with evidences for mutual recognition.

6.6 General requirements on RAMS documentation

A RAM Plan and a Safety Plan shall be established identifying the documents recording information relevant to RAMS throughout the life cycle of the system under consideration.

A process for the maintenance of RAMS documentation shall be defined or referenced in the RAM Plan and Safety Plan.

For each document, traceability shall be provided in terms of a unique reference number (including version) including a defined and documented relationship with other documents.

Each RAMS document and deliverable shall be placed under configuration control from the time of its first release.

Any changes to documents under configuration control shall be recorded.

All documents shall have a list of defined acronyms and abbreviations. Where there are differences in meaning due to historical reasons inside a given document, the different meanings shall be listed and the references given.

If documents from pre-existing systems, products or processes do not fulfil this subclause, it still shall be ensured that these documents are adequately linked to the new documentation, including applicable conditions. Any contradictions shall be addressed and whenever applicable the priority level of the documents used shall be indicated.

The contents of all documents shall be recorded in a form appropriate for handling, processing and storage.

Documents may be combined or divided in accordance with requirements of this clause. Where any alternative life cycle or documentation structure is adopted it shall be established that it meets all the objectives and requirements of this European Standard.

When documents which are produced by different roles as defined in 6.4 are combined into a single document, the relation of parts produced by any independent role shall be traced within the document.

If documents have a hierarchical relationship:

a) There shall be no contradictions to the preceding document;

b) the relevant document should contain or implement all applicable conditions and requirements of the preceding document with which it has a hierarchical relationship.

Whenever the cascading of references is applied, it should consider the increased complexity of verification and validation.

Large volumes of detailed information need not to be included in the RAMS documents, provided that reference, title, purpose and scope of application of referenced documents are given.

In this standard, some documents are mentioned several times in the life cycle description. This is meant to emphasize that an update of the document might be necessary depending on the outcome of the respective life cycle phase. There is no need to produce separate versions of the document in every instance.

6.7 Verification and Validation

6.7.1 Introduction

This European Standard addresses verification and validation tasks in the context of RAMS. Nevertheless, these tasks should be an integral part of the overall system verification and validation tasks.

6.7.2 Verification

In this European Standard, verification tasks are included within each life cycle phase. Verification tasks support and provide input to the validation.

The objective of verification is to demonstrate that the the requirements of each life cycle phase have been fulfilled.

In each life cycle phase as described in Clause 7 of this European Standard, the verification of the activities and deliverables for compliance with the requirements of related life cycle phase defined in this European Standard shall be conducted.

In each life cycle phase, the verification tasks shall deal with:

a) correctness and adequacy of the RAMS analysis, where specified;

b) compliance of the deliverables of the phase with the deliverables of former phases;

c) adequacy of the methods, tools and techniques used within the life cycle phase, where specified;

d) correctness, consistency and adequacy of test specifications and executed tests, as appropriate.

Errors or deficiencies found may require the re-application of some or all of the activities of one or more previous life cycle phases.

6.7.3 Validation

Validation activities are undertaken as follows:

– In life cycle phase 4 “Specification of System Requirements”, validation has the aim to assure that system requirements (including RAMS requirements) have been properly specified applying the requirements defined in this standard and any additional specific requirements defined by applicable legal framework.

– In life cycle phase 9 “System Validation”, validation has the aim to assure that the system under consideration meets the specified requirements for the intended use or application.

Validation can additionally depend on specific requirements defined by applicable legal regulations.

Responsibility of the different validation activities depends on contractual or legal framework. The stakeholders responsible of the validation process along the system life cycle shall always be explicitly defined.

NOTE Validation provided in phase 4 of the life cycle is generally in the scope of railway duty holders, whilst validation provided in phase 9 of the life cycle can be in the scope of the manufacturer/supplier.

RAMS Validation deliverables shall be produced in life cycle phase 4 “System Requirements Specification” and life cycle phase 9 “System Validation”. The inputs for these deliverables shall be provided from tasks in previous phases of the lifecycle.

Throughout the lifecycle of the system under consideration, the involved Validation Entity shall fulfil independence requirements (see EN 50126-2:2017, Clause 7).

Validation shall demonstrate that the process for the system under consideration, including related lifecycle outputs of related life cycle phases, are such that:

– the RAMS requirements for the system under consideration, including safety related application conditions, have been properly specified for the intended use or application;

– the system under consideration, including safety related application conditions, fulfils the related RAMS requirements for the intended use or application.

Validation scope, objectives and activities shall be specified in a Validation Plan.

RAMS management process description may be included in the Validation Plan or in a dedicated RAM / Safety Plan. Depending on the outcome of the Risk Assessment activities and tailoring process (see 6.5) the extent of applicability of the RAMS management process shall be defined and justified.

The Validator shall be entitled to require or perform reviews, analyses and tests.

The Validation Plan for RAMS shall outline or reference:

a) the planning of the specific validation tasks for each phase of the lifecycle as required in Clause 7;

b) a summary justification of the validation strategy chosen. The justification should include consideration of:

- testing strategy;

- acceptance of proposed test strategies by the test entity;

- witness and coverage of the test strategy;

c) the steps necessary to demonstrate the adequacy of the specification of the system, subsystem, equipment to be validated, in fulfilling the requirements for the system, subsystem, equipment. For the requirement of the system, subsystem, equipment the following should be defined:

- the techniques and measures used;

- test and/or analyses used and how their results will be reported;

- management of deviations between expected and actual results of the tests and/or analyses;

- management of non-compliances and safety constraints arising from the deviations;

- management of conditions and constraints derived from the deviations, and how they will be considered in the next lifecycle tasks in terms of the impact on the future life cycle tasks and traceable to the deviations;

d) the steps necessary to demonstrate the adequacy of the tests and/or analysis as a complete set of tests and/or analyses with which the fulfilment of the requirements related to a system/subsystem and/or component can be demonstrated. Non fulfilment and deviations shall be identified.

6.8 Independent Safety Assessment

6.8.1 Objectives

Independent safety assessment is an important means to provide additional confidence about the avoidance of systematic failures of the system under consideration which can adversely influence safety.

Independent safety assessment includes an evaluation and judgement that specified aspects of the safety management process have been adequately undertaken and/or specific requirements with regard to the system or part of the system are fulfilled.

Independent safety assessment is also based on the evaluation of the verification and validation already undertaken. This standard does not define in which cases independent safety assesssment is required.

This standard defines the objectives and the requirements which apply, if independent safety assessment is performed.

NOTE 1 Independent safety assessment can be requested and detailed by technology specific or sector specific standards, or it can be a contractual requirement.

NOTE 2 Independent safety assessment can be required also by the legal framework.

6.8.2 Activities

The content and scope of all independent safety assessment activities shall be described in an independent safety assessment plan developed by the entities responsible for the assessment in cooperation with the remitter and be based on the system definition and the system/subsystem and/or component requirements specification. This plan shall include:

- remit(s) (objective and scope) of the independent safety assessment activities;
- detail of the activities throughout the independent safety assessment process and their link to engineering or operational activities;
- development items (incl. documents) to be taken into consideration;
- statements on pass/fail criteria and the way how to deal with non-conformance cases;
- requirements with regard to content and form of the independent safety assessment documentation.

Each independent safety assessment shall:

- meet the independent safety assessment plan;
- establish an understanding of the process or system, subsystem, equipment within the defined environment;
- assess the adequacy and completeness of the RAMS Validation Plan regarding safety;
- evaluate the conformity of the process and the developed outcomes according to the requirements and activities defined in this European Standard, considering also the verification and validation already undertaken;
- identify and evaluate any deviations from the requirements given in the independent safety assessment remit;
- give a judgment on the acceptability of the safety justification (including deviations) given by the project in the Safety Case described in section 8. This includes the checking that required constraints are captured in safety-related application conditions and are sufficient to control the risk;
- carry out inspections on the overall system development process as appropriate at various phases of development and may ask for additional verification and validation work within the remit of the independent safety assessment;
- provide records of the independent safety assessment activities.

For the fulfilment of these items the entity performing the independent safety assessment shall have access to the system development process and all project related documentation.

The independent safety assessment report:

- shall identify all assessed items of the system under consideration;
- shall record the results of the independent safety assessment;

- shall provide a conclusion;
- may provide recommendations.

A system/subsystem and/or component with an existing independent safety assessment shall be assessed for safe integration into the new working system under consideration and related environment.

The independent safety assessment shall be carried out by an entity who meets the requirements defined in EN 50126-2:2017, Clause 7.

NOTE The legal framework can impose additional independence requirements (e.g. according to EN ISO/IEC 17020).

In the case that the legal framework requires other kinds of safety assessment against specific regulations for authorization it may be combined with the independent safety assessment specified in this standard by assigning a respectively qualified assessor.

Existing documents (i.e. generic independent safety assessment plans) or procedures may be reused if they fit to the requirements for the system under consideration.

The independent safety assessment shall produce the following main deliverables:

- independent safety assessment plan;
- record of the independent safety assessment findings;
- independent safety assessment report.

7 RAMS life cycle

7.1 General

This clause details objectives, requirements, and deliverables for RAMS activities to be undertaken throughout each life cycle phase.

NOTE 1 The life cycle phases are introduced and explained in 6.1.

NOTE 2 General requirements for verification and validation are provided in 6.7.

NOTE 3 Requirements for independent safety assessment activities are provided in 6.8.

NOTE 4 Examples of methods, tools and techniques appropriate for RAMS engineering dependable systems are presented in other standards (see A.4).

NOTE 5 Requirements about adapation of scope and applicability of the requirements (tailoring), to meet the particular needs for the system under consideration are provided in 6.4. The life cycle can be simplified (by tailoring) since a variety of processes and documents can be reused and the activities can focus on the deviations to the original system.

In case of redesign, retrofit or modification, all impacts on Reliability, Availability, Maintainability and Safety shall be identified. An impact analysis shall be undertaken in order to decide how the life cycle needs to be tailored.

7.2 Phase 1: Concept

7.2.1 Objectives

The objective of this phase is to develop a sufficient understanding of the system to ensure a proper performance of all subsequent RAMS life cycle activities.

7.2.2 Activities

In the context of RAMS performance, the following aspects should be analysed:

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

b) the environment of the system, including:

– physical issues;

– system interface issues;

– legislative and economic issues (if they can have impact).

c) previous RAMS requirements and past RAMS performance of similar and/or related systems;

d) current RAMS policy and targets of the relevant railway duty holders;

e) safety legislation.

The scope of the RAMS management requirements for subsequent system life cycle RAMS tasks shall be defined.

7.2.3 Deliverables

The results of the activities of this life cycle phase shall be documented and include any assumptions and justifications made during this life cycle phase.

7.3 Phase 2: System definition and operational context

7.3.1 Objectives

The objectives of this life cycle phase are:

a) define the system and its mission profile;

b) define the boundary of the system;

c) establish the operational requirements influencing the characteristics of the system;

d) define the scope of system risk analysis;

e) establish the initial RAM plan for the system;

f) establish the initial Safety plan for the System;

g) define the functions to be provided by the system;

h) define the organisation for RAM and safety management of the system

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

Guidance on System Definition is given in Annex D of this European Standard.

7.3.2 Activities

7.3.2.1 General

Before any analysis relating to RAMS is undertaken (e.g. hazard identification), boundaries and functions of the system under consideration shall be established. Therefore, at least the following issues shall be outlined:

a) the system objective (intended purpose) and its mission profile, including:

– description of the system under consideration, including system functions and elements which are to be included and system functions which are to be excluded in the analysis;

– long term operating strategy and conditions;

– long term maintenance strategy and conditions;

– system life-time considerations;

– logistic considerations;

b) the system boundary, including:

– interfaces and interactions with physical environment (e.g. climatic conditions, mechanical conditions, altitude) and with other systems;

– interfaces and interactions with other technological systems;

– interfaces and interactions with humans;

– interfaces and interactions with other railway duty holders;

In addition to the functional interfaces, the location(s) of the system parts and their interfaces can influence neighbouring systems and environment.

c) the scope of operational requirements influencing the system, including:

– constraints imposed by existing infrastructure;

– system operating conditions and constraints;

– system maintenance conditions;

– logistic support considerations;

– review of past experience data for similar systems;

– Influence on operational and maintenance personnel, passengers and public, or how they are prevented;

– the description of operating procedures, identification of personnel permitted to carry out these actions and indication of the skills, qualifications and time-resources required, if part of the system operating conditions and constraints;

– if no human activities have been included in the analysis, the reasons for this should be stated;

– the different modes of operation (i.e. normal, abnormal/degraded, maintenance mode), states and transitions and their interactions, if they could have an impact on the systems functionality and safety;

d) existing safety measures and assumptions that determine the limits for the risk assessment;

e) identification of the system and related documents, including assumptions made about particular functions or subsystems that are different from an existing reference version, explicitly stating and justifying the deviations.

For software related items it is clear that software cannot be studied alone. Only through a consideration of the software loaded into a system operating within a certain environment and fulfilling a certain function is it viable to provide a comprehensive system definition.

A RAMS policy shall be established which shall include a policy for resolving conflicts between safety and other aspects like availability, reliability, etc.

An organisation shall be established which shall allocate the roles, responsibilities, competencies, independencies and relationships of organisations undertaking RAMS tasks within the life cycle process. This shall also serve to resolve conflicts as indicated above.

A process for on-going consideration of safety issues and the communication of relevant system safety requirements between the stakeholders should be established. This includes the review of the adequacy of the safety requirements if new findings call for reconsiderations.

7.3.2.2 RAM Plan

The RAM plan for the remaining life cycle tasks shall be established, reviewed and maintained throughout the life cycle of the system. The RAM plan 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 plan should be agreed by the railway duty holder and the railway suppliers for the system under consideration.

NOTE A preliminary RAM analysis can be performed to support targets. This is recommended at least for high risk projects.

The RAM plan shall define the management arrangements to achieve the RAM requirements. This includes details of the policy and strategy to be applied, the scope of the plan and the planning of the RAM activities.

The RAM plan shall include the following:

a) management, including details of:

– the system life cycle and RAM tasks and processes to be undertaken within the life cycle;

– a Failure Reporting Analysis and Corrective Action System (FRACAS) to be applied to the system under consideration from life cycle phase 7 (by the railway duty holder and/or the railway suppliers, as appropriate and agreed between the stakeholders) with records including, e.g:

  • technical data on system;

  • maintenance action;

  • reporting and corrective action.

– all RAM related deliverables from the life cycle;

– RAM acceptance tasks;

– constraints and assumptions made in the RAM plan;

– subcontractor management arrangements;

b) reliability, including:

– reliability analysis and prediction;

– reliability planning;

– reliability testing;

– reliability data acquisition and assessment;

c) availability, including:

– availability analysis;

– sensitivity analysis;

– availability data acquisition and assessment;

d) maintainability, including:

– maintainability analysis and prediction;

– maintainability planning;

– logistic support evaluation.

The RAM plan is considered as a living document. If some content from the above list is not fully available in this early life cycle phase, this information may be added in later life cycle phases.

7.3.2.3 Safety Plan

The Safety Plan for the system shall be established. The Safety Plan shall be implemented, reviewed and maintained throughout the life cycle of the system. Thus it is necessary to define the relationship between the involved stakeholders.

The Safety Plan shall define the following safety activities:

a) the policy and strategy for achieving safety;

b) the scope of the plan;

c) planning of the safety activities;

d) the underlying system life cycle as well as the safety analysis, engineering processes and relationship with assessment to be applied during the life cycle, 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 acceptance criteria and reviewing risk acceptance;

– reviewing the effectiveness of risk reduction measures;

– the establishment and on-going review of the adequacy of the safety requirements;

– system design;

– verification;

– validation to achieve compliance between system requirements and realisation;

– achievement of compliance of the management process with the safety plan (e.g. confirmed via audits);

– safety assurance during the parameterisation of the system (safety classification of the configuration parameters, safety confidence in the parameterisation process and tools used).

e) details of all safety-related deliverables from the life cycle phases, including:

– documentation;

– hardware;

– software;

f) a process to prepare the safety case, considering the hierarchy between system safety activities and documentation;

g) a process for the safety approval of the system including the interface to the railway duty holder and the safety authority;

h) a process for analysing maintenance performance and operation to ensure that safety is not compromised by deviations in assumed operation and maintenance;

i) a process for the maintenance of safety-related documentation;

j) a process for management of the hazard log;

k) interfaces with other related programmes and plans;

l) constraints and assumptions made in the plan;

m) subcontractor management arrangements;

n) periodic safety audit, safety assessment and safety review, throughout the life cycle and appropriate to the safety relevance of the system under consideration, including any personnel independence requirements.

The Safety plan is considered as a living document. If some content from the above list is not fully available in this early life cycle phase or if it changes in a later life cycle phase, information may be added in later life cycle phases.

NOTE Annex A of this standard provides an example outline procedure for the definition of a RAM/safety plan, based on the requirements of this standard. Annex A is informative and for guidance only, and has been populated using the rolling stock system as an example.

7.3.3 Deliverables

The results of this life cycle phase shall be documented, including:

a) a system definition;

b) a RAM plan;

c) a safety plan.

This documentation shall include any assumptions and justifications made during this life cycle phase.

7.4 Phase 3: Risk analysis and evaluation

7.4.1 Objectives

The objectives of this life cycle phase are to:

a) identify and classify hazards / RAM equivalents associated with the system;

b) select risk acceptance principles (RAP);

c) define and apply risk acceptance criteria (RAC);

d) assess risks;

e) establish a process for on-going risk management.

NOTE RAM equivalent to hazard is a condition that could lead to commercial loss related to RAM.

For the reason of simplification, the life cycle representation in this standard shows risk analysis as a one time activity in the early stage of a project. At this stage, for some aspects of the risk analysis only estimations can be made because the detailed design of the product, system or process is not yet available and analysed. This early risk analysis serves as a basis for defining the risk based RAMS system requirements (see life cycle phase 4, 7.5).

Afterwards, an on-going risk management shall be conducted in order to make sure that the risks associated with the system, subsystem, equipment are controlled.

Any analysis produced during the process should include or refer to:

1) the limits of any analysis carried out;

2) assumptions made during the analysis;

3) confidence limits applying to data used within the analysis;

4) the methods, tool and techniques used.

7.4.2 Activities

7.4.2.1 Risk assessment

Risk assessment for the system under consideration, includes also the system definition phase (life cycle phase 2) and shall be be undertaken in accordance with the requirements given in 6.3. Risk assessment comprises risk analysis and risk evaluation.

Risk analysis, using qualitative, quantitative or hybrid approaches, is a systematic and structured process for

1. identifying the undesired events that can lead directly or indirectly to losses during the operation and maintenance of a system. In the context of railway operations, losses could mean harm to passengers, workers or members of the public, harm to the environment or commercial losses related to RAM;

2. identifying the causes, e.g. the component, subsystem or system failures, physical effects, which, perhaps combined with human errors or operational conditions, can result in losses;

3. identifying the control measures that are in place to control or limit the occurrence of each undesired event whose associated risk is not acceptable;

4. in case of explicit risk estimation, estimating the frequencies at which undesired events can occur and estimating the consequences that could occur for the different outcomes that may follow the occurrence of a loss. This would include identifying, where risk reduction is necessary and which control measures shall be in place to control or limit:

– the frequency of occurrence of the undesired event after identification of causes and triggering event, and

– the consequences of the related losses.

If feasible and practicable, the best approach to control a risk is elimination. However this often cannot be achieved and reduction of frequency of undesired events or their consequence are applied. A safety-related example of a relationship of cause, hazard and accident is shown in Figure 10. It can be adapted to RAM aspects correspondingly.

5. determining the additional measures to apply that are required to ensure that the risk is mitigated to levels accepted within the applicable legal framework by the applicable entity (e.g. it satisfies the defined risk acceptance criteria or legal requirements);

6. providing clear and comprehensive documentary evidence of the methodologies, assumptions, data, judgments and interpretations used in carrying out the risk analysis.

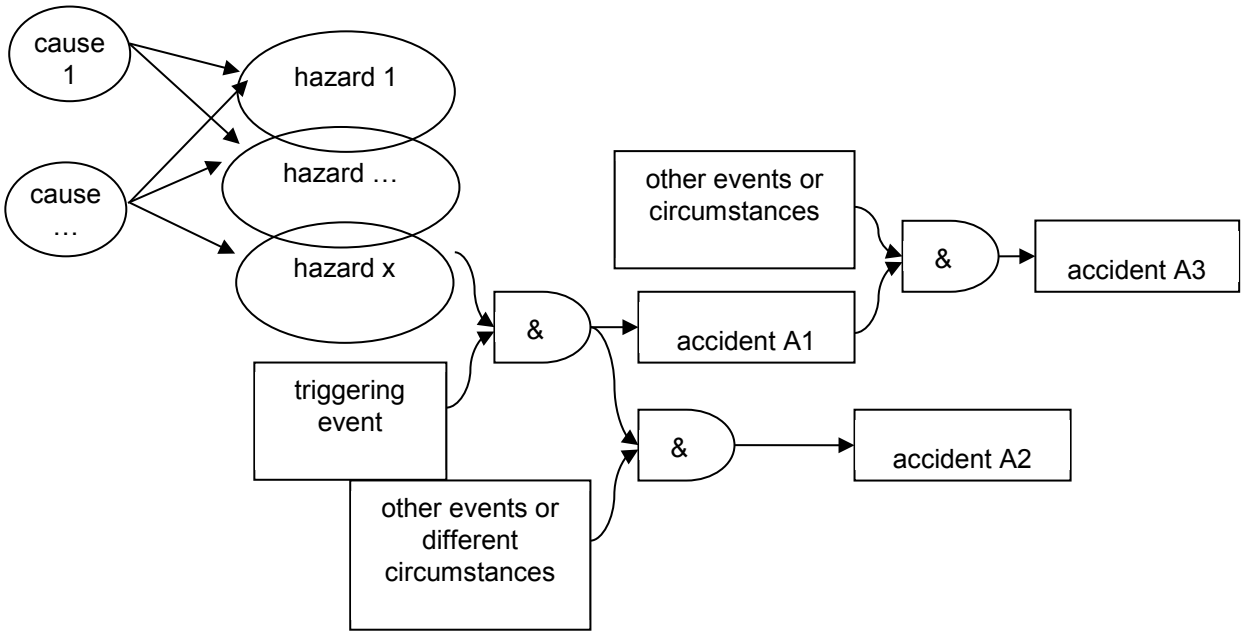


Figure 10 — Relationship of cause, hazard and accident

It is important to note, that given safety targets referring to frequency categories should be related to the item under consideration (an instance of the function or system under consideration), but not to the sum of items in use or intended to be used. In other words not to the “fleet” of them, but to the single instance of this function or system. Otherwise compliance to a safety objective could require revising a system in case additional identical equipment will be put into operation.

EXAMPLE 1: The frequency categories could apply to:

– a door system (per door);

– a brake system (per independent braking unit);

– a single signal;

– a main switch in a power supply station.

It is important to note however that there can be different consequences when losing a single system, or multiple instances of the same system. In such case, system safety requirements are to be specified for all accident scenarios.

EXAMPLE 2: A single door opening when the train is running might trigger a fatality.

EXAMPLE 3: All doors opening when the train is running might however trigger multiple fatalities. This means that the overall control command function could have a more stringent safety target than the local function.

All reasonably foreseeable hazards / RAM equivalents associated with the system in its application environment shall be systematically identified. This activity should include hazards and their RAM equivalents arising from:

a) system normal operation;

b) system fault conditions;

c) system emergency operation;

d) foreseeable system misuse, excluding deliberate misuse;

e) system interfaces;

f) system functionality;

g) system configuration parameters;

h) system operation, maintenance and support issues;

i) system disposal considerations;

j) human factors;

k) occupational health issues;

l) mechanical environment;

m) electrical environment;

n) natural environment to cover such matters as snow, floods, storms, rain, landslides etc.

For the purpose of hazard / RAM equivalents identification it is beneficial to use a structured list. This list serves as a basis and is non-exhaustive. If used, it should be checked against the application and amended if necessary.

The relationships of hazards / RAM equivalents to related consequences shall be defined, identifying combination and sequence of contributing events.

The identified hazards shall be classified based on expert judgement at least into those associated with broadly acceptable risk(s) and those associated with risks that are not considered as broadly acceptable. Details on expert judgement can be found in EN 50126-2.

Hazards associated with a broadly accepted risk need not be analysed further but shall be registered in the hazard log.

NOTE For further information about criteria for ”broadly acceptable”, it is advised to refer to 6.3.

Risk acceptance principle to be applied shall be selected:

- use of code of practice;
- use of a similar system as a reference;
- explicit risk estimation (qualitative or quantitative).

In case of explicit risk estimation, risk acceptance criteria shall be defined.

Details with regard to the use of risk acceptance principles can be found in EN 50126-2.

The risk to the system for each hazard / RAM equivalent shall be evaluated against the previously defined risk evaluation and acceptance criteria.

Depending upon the risk acceptance principle selected, it can be necessary to estimate the impact of different scenarios (including different triggering events) to help inform the decision about the acceptability of the risk during the risk evaluation.

7.4.2.2 Hazard Log

A hazard log shall be established as the basis for on-going risk management for safety. It represents a tool to track hazards and their closure. The hazard log shall be updated throughout the life cycle whenever a change to identified hazards occurs or a new hazard is identified. The hazard log shall include or refer to details of:

a) the purpose of the hazard log;

b) each hazard, entities responsible for managing the hazard, and the contributing functions or components;

c) likely consequences and frequencies of the sequence of events associated with each hazard, when applicable;

d) the risk arising from each hazard (in quantitative or qualitative terms), where appropriate;

e) risk acceptance principles selected and in case of explicit risk estimation also the risk acceptance criteria to demonstrate the acceptability of the risk control related to the hazards;

f) for each hazard: the measures taken to reduce risks to a tolerable level or to remove the risks;

g) exported safety constraints.

There can be several types of hazard logs; e.g. internal ones (for managing the company's internal processes) and external ones, called external hazard log. An external hazard log is an extract of the hazard log that is suitable for transferring information between stakeholders. It aims to inform other stakeholders about the relevant safety aspects at the interfaces to their systems or subsystems and about hazards which cannot be controlled by one stakeholder alone.

NOTE The external hazard log can also be called "hazard record".

7.4.3 Deliverables

The results of this life cycle phase shall be documented, including:

a) the risk assessment;

b) the hazard log;

c) updated safety plan (if appropriate);

d) updated RAM plan (if appropriate);

e) establish indipendent safety assessment plan (if appropriate).

This documentation shall include any assumptions and justifications made during this life cycle phase.

7.5 Phase 4: Specification of system requirements

7.5.1 Objectives

The objectives of this life cycle phase are to:

a) specify the overall RAMS requirements for the system under consideration;

b) specify the overall demonstration process and criteria for acceptance of RAMS of the system;

c) provide a comprehensive and identified set of requirements for the subsequent life cycle phases;

d) specify necessary monitoring requirements according to the process for analysing operation and maintenance performance arranged in the Safety Plan (that enable the system to perform the required tasks in life cycle phase 11).

7.5.2 Activities

The overall RAMS requirements for the system shall be specified on the basis of the system definition of sub-clause 7.3 and the risk analysis and evaluation of sub-clause 7.4. The RAMS requirements for the system under consideration shall include:

a) functional requirements and supporting performance requirements, including safety functional requirements and associated safety target for each safety-related function;

b) logistic support requirements;

c) interfaces;

d) application environment and mission profile;

e) tolerable risk levels for the consequences arising from the identified hazards, when applicable;

f) external measures necessary to achieve the requirements;

g) system support requirements;

h) details of the limits of the analysis;

i) details of any assumptions made;

j) identification of technology related standards;

k) scope of diagnosis and monitoring, specifically requirements for the monitoring of the effectiveness of the proposed safety measures.

The requirements should be expressed and structured in such a way that:

l) they are complete, precise, unambiguous, verifiable, testable and maintainable;

m) they are written to aid comprehension by those who are likely to utilise the information at any stage of the system life cycle;

n) they are expressed in natural or formal language and/or logic, sequence or cause and effect diagrams. The requirements should define the necessary functions with each function being individually defined;

o) the defined set of requirements is suitable to define a system that is fit for the intended purpose.

The overall requirements for achieving compliance with RAMS requirements for the system shall be specified, including:

p) acceptance criteria for the overall RAMS requirements;

q) a demonstration and acceptance process for the overall RAMS requirements supported by the system RAMS validation plan.

NOTE Guidance on specification of system safety system requirements can be found in EN 50126-2.

The Safety Plan and the RAM plan shall be updated (if appropriate) to ensure that all planned tasks are consistent with the system's emergent RAMS requirements.

When necessary, assumptions supporting definition of safety requirements shall be identified as safety-related application conditions for the future life cycle tasks operation, maintenance and decommissioning.

7.5.3 Deliverables

The results of this life cycle phase shall be documented, including

a) the RAMS system requirements specification;

b) Safety-Related Application Conditions (if appropriate);

c) updated hazard log (if appropriate);

d) updated safety plan (if appropriate);

e) updated RAM plan (if appropriate);

f) the Validation Report covering phases 1 to 4;

g) RAM validation plan for the subsequent phases;

h) Safety validation plan for the subsequent phases.

This documentation shall include any relevant assumptions and justifications made during this life cycle phase.

7.5.4 Specific validation tasks

General requirements for validation tasks are described in 6.7.3.

In this life cycle phase, a Validation Report shall be established including:

a) identification and name of:

- the system under consideration;

- the documents and other items used for the validation;

- processes, technical support tools and equipment used if any;

- the simulation models used if any;

b) confirmation that process and activities have been conducted according to what has been described in the safety plan. Deviations from the safety plan shall be recorded and justified;

c) validation of the system safety requirements against the risk assessment processes conducted until the end of lifecycle phase 3, see 7.4;

d) validation of the RAM system requirements against specified RAM targets and RAM policies of the railway duty holders;

e) confirmation that all system requirements (including RAMS, functional, and external legal requirements) are adequately analysed and specified in order to allow the system under consideration to serve the intended use.

In this life cycle phase, a Validation Plan for the achievement of the specified RAMS requirements for the system under consideration shall be established.

7.6 Phase 5: Architecture and apportionment of system requirements

7.6.1 Objectives

The objectives of this life cycle phase are to:

a) apportion the system RAMS requirements to the designated subsystems and/or components;

b) design subsystems and components that work together as a system which fulfils the required functions at the system level;

c) describe the RAMS requirements and specify the interfaces for all subsystems and components derived from the RAMS requirements (which prepares later integration activities);

d) define the acceptance criteria to demonstrate fulfilment of the RAMS requirements for the system, subsystem, equipment in subsequent lifecycle phases;

e) identify and evaluate the significance of the interactions between the subsystems.

NOTE Interactions can be defined at different abstraction levels. Such interactions can be described in interface specifications.

7.6.2 Activities

A system architecture shall be developed and defined that fulfils the RAMS requirements. The architecture shall be based on a structured decomposition into subsystems and/or components with completely defined interfaces between the subsystems and/or components. For each subsystem or component a set of RAMS requirements shall be allocated which is derived from the system requirements and from the design in sufficient depth. To achieve this, a structured design methodology shall be applied.

The system architecture should be expressed and structured in a way that it is clear, precise, unambiguous, verifiable, testable, maintainable and feasible. It should aid the comprehension by those who are likely to utilise the information at any phase of the life cycle and be traceable to the system requirement.

Particular attention is required for the specification of RAMS requirements for the control of interfaces where safe and reliable interaction can be compromised. Constraints on the choice of technology (i.e. independence of functions or processes of development) shall be identified. All safety-related assumptions made during the development of the system architecture shall be specified and documented.

The designated subsystems and/or components shall be specified to achieve the system RAMS requirements, including the impact of common cause and multiple failures.

If new hazards are identified arising from the architecture, requirements to control these hazards shall be derived from the new hazards and allocated to the related subsystems and/or components.

If pre-existing subsystems and/or components are used to fulfil system requirements it shall be ensured additionally that the requirements for integration of the pre-existing subsystems and/or components are clearly identified and fulfilled.

It should be possible to use COTS equipment, provided that evidence of the quality is given. For safety related applications, at the system level, it shall be demonstrated that possible failures from the COTS products will not jeopardize the defined safety requirements, e.g. controlled by the architecture of the system (integration issue).

In cases where safety-related functions are developed according to a code of practice, the relationship of these functions to the used code of practice shall be given and justified in the system architecture.

The realisation of safety-related functions shall be performed in accordance with the related code of practice.

Acceptance criteria, acceptance processes and procedures, as well as demonstration for subsystems and/or components including their interfaces, shall be specified to ensure compliance with the subsystem and/or component requirements.

The Safety Plan, RAM plan and the RAM and Safety Validation Plan shall be updated (if appropriate) to ensure that all planned tasks are consistent with the system's emergent RAMS requirements following the apportionment.

NOTE Key areas of concern include requirements for personnel independence and the control of system interfaces where safety functionality can be compromised.

Safety-Related Application Conditions for the future tasks in life cycle phases Operation, Maintenance and Decommissioning shall be derived from the RAMS analysis of the system under consideration performed in this life cycle phase.

7.6.3 Deliverables

The results of this life cycle phase shall be documented, including:

a) system architecture (structure of decomposition into subsystems etc.) including interface specifications and system hazard analysis (architecture and hazard analysis of subsystem and components);

b) allocation of RAMS requirement specification to subsystems and/or components;

c) Acceptance Criteria and demonstration and acceptance processes and procedures;

d) updated safety plan (if appropriate);

e) updated RAM plan (if appropriate);

f) updated RAM Validation Plan (if appropriate);

g) updated Safety Validation Plan (if appropriate);

h) updated Safety-Related Application Conditions (if appropriate);

i) updated hazard log (if appropriate).

This documentation shall include any assumptions and justifications made during this life cycle phase.

7.7 Phase 6: Design and Implementation

7.7.1 Objectives

The objectives of this life cycle phase are to:

a) create subsystems and components conforming to RAMS requirements;

b) demonstrate subsystems and components conform to RAMS requirements;

c) refine plans for future life cycle tasks involving RAMS.

7.7.2 Activities

The subsystems and components shall be designed to meet the RAMS requirements.

The design of the subsystems and components shall be implemented to meet RAMS requirements.

The RAMS tasks of further life cycle phases shall be refined. These phases shall include:

– Integration;

– Operation and maintenance;

– Performance monitoring (if applicable /could also be contractually agreed).

Operation and maintenance procedures shall be prepared. These procedures shall include all the relevant information for providing spare parts, particularly items in safety-related functions.

Training measures for operation and maintenance staff including training material shall be defined.

Manufacturing process capable of producing RAMS-validated subsystems and components shall be prepared with the relevant activities defined in the safety plan for this purpose.

The following aspects should be considered:

– environmental stress screening;

– RAM improvement testing;

– inspection and testing for RAMS-related failure modes.

A process for the integration into the system, that ensures for subsystems and components the RAMS conformity, shall be defined. Safety-related activities for this purpose are part of the Safety Plan.

The following aspects should be considered:

– measures to prevent installation errors;

– testability of installed subsystems and components;

– activities, defined in the safety plan, which are relevant to this life cycle phase.

A RAM analysis shall be performed,

A hazard analysis for safety purposes shall be performed.

A safety case shall be prepared, justifying that the system under consideration, as designed, meets the safety requirements. The contents and documentation structure of the safety case shall follow the requirements stated in 8.2.

The RAMS Validation Plan shall be updated (if appropriate) to ensure that all planned tasks are consistent with the system's emergent RAMS requirements following the design.

Installation and commissioning procedures shall be prepared.

Safety-Related Application Conditions and limitations for the future tasks in life cycle phases Operation, Maintenance and Decommissioning shall be derived from the deviations, which are identified in this life cycle phase.

7.7.3 Deliverables

The results of this life cycle phase shall be documented, including:

a) RAM analysis;

b) Hazard analysis;

c) updated Safety-Related Application Conditions (if appropriate);

d) updated hazard log (if appropriate);

e) installation and commissioning procedures;

f) operation and maintenance procedures;

g) training measures;

h) plan(s) for further life cycle tasks;

i) updated RAM plan (if appropriate);

j) updated safety plan (if appropriate);

k) updated RAM Validation Plan (if appropriate);

l) updated Safety Validation Plan (if appropriate);

m) safety case(s) (if appropriate).

NOTE The Safety Case preparation is an implicit deliverable of the objective of safety demonstration.

This documentation shall include any assumptions and justifications made during this life cycle phase.

7.7.4 Specific verification tasks

The following verification tasks shall be undertaken within this life cycle phase in addition to those tasks required in 6.7.2:

a) verification that subsystem and component design complies with the RAMS requirements;

b) verification that subsystems and components implementation complies with design;

c) verification that the manufacturing arrangements produce RAMS-validated subsystems and components;

d) verification that all future life cycle activity plans are consistent with RAMS requirements for the system.

NOTE Verification is based on results of analyses and tests.

7.8 Phase 7: Manufacture

7.8.1 Objectives

The objectives of this life cycle phase are to:

a) manufacture the subsystems and components;

b) establish and apply RAMS-centred assurance arrangements.

7.8.2 Activities

The manufacturing process prepared in life cycle phase 6 shall be implemented and operated.

RAMS-centred assurance arrangements shall be established, including:

a) quality assurance measures suitable to meet RAMS requirements;

b) manufacturing process improvement and assurance measures as applicable;

c) environmental stress screening as applicable;

d) inspection and testing for RAMS-related failure modes.

Safety-related application conditions for the future life cycle tasks of operation, maintenance and decommissioning shall be derived from the deviations identified in this life cycle phase.

7.8.3 Deliverables

The results of this life cycle phase shall be documented, including RAMS related aspects of:

a) quality assurance reports (regarding manufacturing process and measures for RAMS);

b) inspection and testing reports;

c) material handling and logistic arrangements;

d) updated hazard log (if appropriate);

e) updated Safety-Related Application Conditions (if appropriate);

f) updated safety case(s) (if appropriate);

g) updated RAM plan (if appropriate);

h) updated safety plan (if appropriate);

i) updated RAM Validation Plan (if appropriate);

j) updated Safety Validation Plan (if appropriate).

This documentation shall include any assumptions and justifications made during this life cycle phase.

7.9 Phase 8: Integration

7.9.1 Objectives

The objectives of this life cycle phase are to:

a) assemble and install the integrated system, total combination of subsystems and components required to form the complete system;

b) demonstrate that integrated system, subsystems and components work together as defined by the interfaces;

c) demonstrate that integrated system, subsystems and components meet their RAMS requirements;

d) initiate system support arrangements.

7.9.2 Activities

The subsystems and components shall be integrated according to the integration planning. The fulfilment of the systems functionality as well as the specified RAMS requirements shall be demonstrated. The integrated system shall be installed into a higher level system. Therefore, the requirements of this life cycle phase shall apply both to the integration of components and subsystems and to the incorporation of a system into the superior system. This could be regarded as a two-tiered integration for which similar activities apply.

In case of modifications or changes introduced to the integrated system, a rollback procedure (i.e. capability to return to the previous release) should be available during integration.

In case of modifications or changes introduced, an impact analysis of the system architecture from life cycle phase 5 shall be performed to ensure that the subsystems interact safely and perform the intended

functions after the modification or change. The impact analysis shall evaluate to which extent previous life cycle activities shall be repeated.

The system shall be tested and analysed in accordance with the system integration planning. These tests and analyses shall show that all subsystems and components of the system interact correctly as specified in the interface specifications to perform their intended function and do not perform unintended functions.

During the integration of the subsystems and components of the system, the fulfilment of all safety-related application conditions defined for those subsystems and components shall be shown. This includes, for subsystems developed according to a code of practice, the evidence for the conformance of the realisation to the used Code of Practice.

Safety-related application conditions inherited from the subsystems and components, which cannot be fulfilled at the technical system level, shall be derived and documented.

Additional system support arrangements related to RAMS aspects shall be initiated, including:

a) start staff training;

b) make system support procedures available;

c) establish spare parts provision;

d) establish tool provision.

Safety-related application conditions for the future life cycle phases operation, maintenance and decommissioning shall be derived from the deviations identified in this life cycle phase.

7.9.3 Deliverables

The results of this life cycle phase shall be documented, including:

a) installation documentation;

b) integration report (if appropriate);

c) action taken to resolve failures and incompatibilities;

d) system support arrangements;

e) updated hazard log (if appropriate);

f) updated Safety-Related Application Conditions (if appropriate);

g) updated safety case(s) (if appropriate);

h) updated RAM plan (if appropriate);

i) updated safety plan (if appropriate);

j) updated RAM Validation Plan (if appropriate);

k) updated Safety Validation Plan (if appropriate).

This documentation shall include assumptions and justifications made during this life cycle phase.

7.9.4 Specific verification tasks

The following verification tasks shall be undertaken within this life cycle phase in addition to those tasks required in 6.7.2:

- evaluation that all SRACs of the integrated subsystems/ components are fulfilled during the integration.

7.10 Phase 9: System Validation

7.10.1 Objectives

The objectives of this life cycle phase are to:

a) confirm by examination and provision of objective evidence that the system under consideration in combination with its Safety-Related Application Conditions complies with the RAMS requirements;

b) confirm or update the safety case for the system under consideration, according to the results of the validation.

7.10.2 Activities

The general requirements on activities to be performed are described in 6.7.3.

Dependent upon the level of the safety integrity for the system under consideration, validation activities shall include also:

– The Hazard Log shall be reviewed and updated to record any residual hazards identified during system validation and to ensure that the risks from any such hazards are effectively managed.

– The safety plan shall be reviewed with regard to its continued applicability.

– The safety case for the system under consideration shall be updated. The safety case shall justify that the system under consideration complies with the system safety requirements.

A probationary period of operation may be undertaken, to resolve potential in-service system problems. In this case, the need for demonstrating system safety shall be considered prior to the probationary operation and non-probationary operation.

A process for the acquisition and evaluation of operational data and maintenance data shall be established and implemented as an input to a system improvement process.

If the system has been subjected to an impact analysis as set out in 7.9.2, adequacy of this analysis shall be evaluated.

Safety-related application conditions for the future life cycle tasks operation, maintenance and decommissioning shall be derived from the deviations identified in this life cycle phase.

Collection of all safety-related application conditions (e.g. in a record) for the future life cycle phases operation, maintenance and decommissioning shall be documented.

7.10.3 Deliverables

The results of this life cycle phase shall be documented, including:

– RAM validation report;

– safety validation report;

– updated hazard log (if appropriate);

– updated safety plan (if appropriate);

– updated safety case (if appropriate);

– updated Safety-Related Application Conditions (if appropriate);

– process for the acquisition and evaluation of operational data.

In this life cycle phase, a Validation Report shall be outlined including:

a) identification and name of:

- the system under consideration;
- the documents and other items used for the validation;
- processes, technical support tools and equipment used, along with calibration data;
- the simulation models used if any.

b) confirmation that the process and activities defined in the validation plan have been met. Deviations from the validation plan shall be recorded and justified;

c) evaluation of the performance and coverage of requirements tracing in development and verification;

d) confirmation that the development and verification have handled corrective actions in accordance with the change management process and procedures and with clearly identified deviations;

e) evaluate the coverage of the requirements for the system under consideration by the tests and/or analyses;

f) identification of the tests defined and executed by the validator if any;

g) evaluate the correctness, consistency and adequacy of the qualification according to the required technology related standards;

NOTE The technology related standards are defined in the system requirements specification.

h) conclusion of the validation results and whether the system under consideration fulfils the safety requirements for its intended use in the defined environment.

The following may be covered by the safety case and the validation report can refer to this document regarding:

– evaluation of the conformity of the development process and of the validated system under consideration against the requirement/activities defined in this European Standard.

– evaluation of the conformity of the development process to the plans (e.g. Safety Plan, Quality management);

– confirmation of the correctness, consistency and adequacy of the verification process (testing, analysis and reviewing) with respect to the planning of the verification and the verification reports;

– identification and classification of all deviations and their relation to the safety-related application conditions derived from those deviations in terms of risk. Taking into consideration external risk reduction measures;

– confirmation of the correctness, consistency and adequacy of installation, commissioning, maintenance and operation manuals for the system under consideration.

7.11 Phase 10: System acceptance

7.11.1 Objectives

The objectives of this life cycle phase are to:

a) assess compliance of the total combination of subsystems, components, their interfaces and Safety-Related Application Conditions with the overall RAMS requirements;

b) accept the system for entry into service.

NOTE In this European Standard, the term system acceptance is used only for technical aspects of the acceptance procedure. Legal aspects of the system acceptance are not considered in this standard. It is advised to clarify the legal aspects of system acceptance between the customer and the supplier in advance.

7.11.2 Activities

All system verification and validation tasks, specifically the RAMS verification & validation and the safety case, shall be assessed in accordance with the defined risk acceptance criteria.

NOTE Risk acceptance criteria are given by contractual agreements or legal framework and were specified in life cycle phase 4.

The results of this assessment shall be recorded in an acceptance report. The acceptance report should include a confirmation that the delivered product, system or process is fit for entry into service.

The following tasks shall be undertaken by the entity which is accepting the system (railway duty holder or other):

a) evaluation of the acceptance report with respect to the defined acceptance criteria;

b) evaluation of the safety plan with regard to its continued applicability including the possible need of Independent Safety Assessment (if applicable);

c) evaluation of the updated hazard log.

7.11.3 Deliverables

The results of this life cycle phase shall be documented, including:

- Independent Safety Assessment Report (if appropriate);
- endorsement of Safety-Related Application Conditions (if appropriate);
- Acceptance report.

This documentation shall include assumptions and justifications made during this life cycle phase.

7.12 Phase 11: Operation, maintenance and performance monitoring

7.12.1 Objectives

The objective of this life cycle phase is to operate, maintain and support the system under consideration such that compliance with RAMS requirements is maintained. This includes continuously monitoring and evaluating the RAMS performance of the system and deriving measures to address shortcomings and to achieve improvements.

7.12.2 Activities

Prior to the start of this life cycle phase the manufacturer should provide to the customer all information necessary to formulate plans and procedures for Operation, Maintenance and performance monitoring, and enable compliance with RAMS requirements to be maintained. This information shall include any Safety-related Application Conditions (SRACs) identified during the course of verification and validation.

The Operation and Maintenance Plans should include the following:

1) An explanation of operational status: The conditions that exist in each system/subsystem/hardware should be defined to provide operating and maintenance personnel with sufficient understanding during the following situations:

a) start-up: this should describe the start-up conditions of the system, subsystem or hardware when power is initially applied, or following shut-down due to power interruption or other cause;

b) normal operation: once the system/subsystem/hardware has successfully completed initialisation, the conditions during normal operation shall be defined;

c) changeover: if the system/subsystem or hardware in which it is configured, has a facility to change over to either a cold or hot standby system/subsystem, then the conditions defined in a) and b) should be re-stated for this changeover routine. The reaction of the system/subsystem or hardware to the changing of failed modules shall also be clearly defined;

d) shut-down: when a system/subsystem or hardware is shut down intentionally for a configuration change or de-commissioning, or unintentionally via a power failure, then all relevant conditions shall be defined.

2) maintenance should be defined in respect of:

a) that undertaken on the system in-situ or at designated routine maintenance facilities;

b) the repair or refurbishment of systems, subsystems or hardware that are no longer in-situ or that is taking place in facilities not classed as routine maintenance facilities, e.g. mid-life overhauls which are undertaken by the customer and the manufacturer;

c) preventative maintenance;

d) corrective maintenance;

e) maintenance aids: for each level of maintenance, the maintenance aids available to personnel should be defined.

3) an analysis of human factors and competence requirements in maintenance that can influence the continued achievement of the required RAMS performance.

4) an analysis of human factors and competence requirements in operation that can influence the continued achievement of the required RAMS performance.

The operation and maintenance procedures shall be implemented, particularly with regard to system performance and life cycle cost issues. This requires considering the product, system or process in its operational environment, e.g. including the application of external risk reduction measures

Compliance with RAMS requirements shall be assured throughout this life cycle phase, by:

a) regular review and update of operation and maintenance plans and procedures;

b) conformity with operational plans and procedures;

c) conformity with maintenance plans and procedures;

d) regular review of system training documentation;

e) regular review and update (if appropriate) of an operational Hazard Log;

f) ensuring compliance to the Safety-Related Application Conditions (SRACs);

g) investigating and handling hazardous incidents and accidents and ensuring rapid response fault finding;

h) for systems undergoing modification, definition and implementation of mitigation actions, if applicable, to ensure the overall integrity of the system until the modification is completed or reported problems are investigated and corrected;

i) conformity with support agreements including logistics, spare parts, repairs, tools, calibration and quality measures to prevent or detect errors occurring during storage and transfer;

j) maintenance of the failure reporting and corrective action system (FRACAS).

NOTE 1 The operational Hazard Log is based on the Hazard Record extracted from the Hazard Log resulting from life cycle phase 10.

The review and updates of the Operation and Maintenance Plan shall include issues raised and addressed during the initial operation and maintenance phase and at applicable stages thereafter.

It shall be implemented a process for:

a) the acquisition of RAMS performance data;

b) recording of RAMS performance data, associated analysis and evaluation as applicable, e.g. by means of a FRACAS.

Throughout the operational lifetime the system baseline shall be recorded and kept traceable under configuration management control.

NOTE 2 This is of special importance when critical faults are discovered and need to be corrected in more than one installation. Manufacturers and maintainers might need to implement complementary arrangements for configuration management, so that the manufacturer can trace the baseline of systems provided to particular customers and individual maintainers can trace the location of individual items.

The FRACAS process is required to continuously provide feedback to the operations safety manager, the designer, manufacturer, operations manager and maintenance manager regarding any failures and defects (and possible causes) found during operational service, Failures will potentially have a variety of causes including component failures, operational errors, maintenance and other errors. It is therefore imperative that the reporting process is clear and logical and that there is a collective forum for all stakeholders to agree the most likely source of failure and hence investigation and corrective actions.

NOTE 3

1) Complementary FRACAS records can need to be kept by different entities. Maintenance organisations might have a generic FRACAS which covers many different types of system for which they are responsible, while manufacturers can have a FRACAS which encompasses systems supplied to a variety of different customers. The manufacturer can be able to diagnose component failures which are not accessible to the maintainer.

2) Referencing of accidents, hazards and causes will preferably be consistent within the safety case and other performance monitoring tools and processes. This will help respective organisations to align issues and identify trends.

The FRACAS shall be maintained throughout the operation and maintenance life cycle. To ensure that priority issues are addressed, the failures and defects should be categorised for both safety and reliability for varying levels of severity/criticality. As a minimum, the FRACAS shall be populated with information about failures and defects identified during operation and maintenance. This information shall include:

a) time of the failure;

b) cause of the failure;

c) detailed description of the failure;

d) corrective action taken;

e) safety ranking for the failure.

f) when and how the failures and defects have been detected (e.g. in operation or during a scheduled maintenance);

g) the effects of the failures and defects up to the railway system level.

The FRACAS records shall be periodically reviewed to determine whether any improvement is needed in the following:

h) Operation and maintenance procedures and manuals;

i) System training documentation;

j) Operational Hazard Log;

k) System design;

l) Human factors aspects of operation and maintenance.

When changes are proposed an impact analysis shall be performed on each change request. The analysis shall include reviewing the impact on:

m) the system/subsystem or hardware operational/functional safety performance;

n) the system/subsystem/hardware interfaces;

o) adjacent system/subsystem or hardware operational/functional safety performance;

p) the modification installation work, with consideration given to adjacent system/subsystem and hardware that can be affected due to systematic failures.

The impact analysis shall result in a decision on which parts of the safety life cycle will be repeated for the modification, all relevant documentation for the effected life cycle steps shall be updated, with equal depth and quality as the original documentation that was produced during the development of the system. The details and results of the modification, risk analysis and testing shall be included in the safety case.

All changes and system/subsystem or hardware identified as being at risk shall be tested for correct operation on completion of the change.

For each identified recommendation a decision shall be taken whether the recommendation shall be realised or not. These decisions shall be justified and recorded.

7.12.3 Deliverables

The results of this life cycle phase shall be documented, including:

a) updated system and support documentation, as appropriate, within this life cycle phase;

b) plans and records suitable to trace the RAMS tasks undertaken within this life cycle phase (e.g. evidence of correct execution of the Operation and Maintenance Plan);

c) reports of RAMS performance analyses and evaluations;

d) identified recommendations and record of associated decisions;

e) updated operational Hazard Log (if appropriate);

f) change request with impact analysis on the re-application of the system life cycle;

g) design specifications and requirements updated, if impacted;

h) system safety case updated as required to include design modification and/or risk analysis (as appropriate);

i) updated Operation and Maintenance plans and processes.

This documentation shall include assumptions and justifications made during this life cycle phase.

7.12.4 Specific verification tasks

There are no specific verification requirements for this life cycle phase in addition to those tasks required in 6.7.2.

7.13 Phase 12: Decommissioning

7.13.1 Objectives

The objective of this life cycle phase is to control RAMS implications of system decommissioning and disposal tasks.

7.13.2 Activities

The RAMS impact of decommissioning and disposal on any relevant external system or facility shall be identified.

The decommissioning shall be planned, including the establishment of procedures for:

a) the safe closing down of the system;

b) the safe dismantling of the system.

As external systems or facilities can be affected, these systems or facilities also need consideration. It shall be taken into account that the disposal can represent a modification of the external system or facility.

7.13.3 Deliverables

The results of this life cycle phase should be documented, including:

- the impact on RAMS associated to the closing/dismantling of the system;

- a Decommissioning report.

This documentation should include any assumptions and justifications made during this life cycle phase.

8 Safety Case

8.1 Purpose of a safety case

The safety case consists of the documented structured safety justification which provides the evidence of how the system under consideration complies with the specified safety requirements, within the defined scope of its proposed use. This:

- allows those who are to use the system to have confidence that the system complies with the specified safety requirements;

- provides a demonstration that the system is in compliance with the specified safety requirements, determined in accordance with the requirements specified in the EN 50126 series;

- provides a basis for independent safety assessment;

- provides the Safety-Related Application Conditions (SRAC).

NOTE A safety case is used to provide one party with assurance from another. In this standard the assurance is ultimately provided from the party developing the system under consideration (e.g. the supplier, or the contracting entity) to the party responsible for operating and maintaining the railway (e.g. Railway Undertaking or Infrastructure Manager).

There are two usual limitations to the scope of a safety case:

- demonstration of correctness of the safety requirements, and related risk assessment, is usually external to the safety case;
- proof of compliance with the Safety-Related Application Conditions (SRAC) identified in the safety case is not usually contained within the safety case itself.

The types of safety case, dependencies and relationship are defined in EN 50126-2:2017, Clause 6.

8.2 Content of a safety case

The safety case shall contain, as a minimum, the following:

1. Definition of the system under consideration. It includes:

– key subsystems/equipment;

– architecture and expected behaviour;

– interfaces and the operational environment;

– safety requirements;

– definition of the configuration/version of the system under consideration to which the safety case applies;

– reference to the input safety requirements as well as the related risk assessment analyses.

2. Quality Management Report. It includes:

– quality management activities and evidence.

3. Safety Management Report. It includes:

– safety management activities and evidence.

4. Technical Safety Report. It includes safety assurance activities and evidence, comprising:

– assurance of safety in fault-free conditions;

– assurance of safety in the event of failures and errors;

– assurance of safety with adverse external influences;

– Safety Related Application Conditions (SRAC).

5. Related safety cases. It includes:

– references to the safety cases of all subsystems/equipment on which the main safety case depends.

– demonstration that all safety-related application conditions specified in each of the related subsystem/equipment safety cases are either fulfilled in the main safety case or carried forward into the safety-related application conditions of the main safety case.

6. Conclusion. It includes:

– Summary of the evidence presented in the previous parts of the safety case;

– list of all specific safety claims, and

– statement that the system under consideration is adequately safe, subject to compliance with the specified application conditions.

Annex A
(informative)

RAMS plan

A.1 General

Annex A gives an example of an outline procedure for developing a basic RAM plan/safety plan and an example of a basic RAMS plan (RAM plan/safety plan). It also lists some methods and tools for RAMS management and analysis.

The supplier should establish a RAMS plan to facilitate meeting the RAMS requirements for the application under consideration.

A.2 Procedure

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

1. Define the appropriate life cycle phases respectively project phases which are in line with the company's business process;

Result: The Company's life cycle or project phases are established

2. Assign to each life cycle or 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 or project 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

A.3 Basic RAMS plan example

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

NOTE The proposed project phases are in complement to life cycle phases defined in Clause 7 and summarised in Table 1.

Table A.1 — Example of a basic RAMS plan outline

Project-Phase	RAMS Tasks	Responsibility	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 (Subsystems/equipment, other relevant systems etc.) Perform system hazard & safety risk analysis Perform RAM related risk analysis Prepare for future RAMS data assessment Clause by 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 plan (Standard RAMS plan sufficient?) Assign RAMS requirements to sub-contractors, suppliers Define RAMS acceptance criteria (overall)		
Order Processing: Design and Implementation	Reliability analysis (e.g. FMEA) Safety analysis (e.g. 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 specific application safety case Initiate RAMS data assessment RAM testing during early operation, data screening and evaluation		

Project-Phase	RAMS Tasks	Responsibility	Reference document
Operation/ Maintenance	Provisional operation and maintenance (Maintenance/repair policy) Operation and maintenance personnel training RAMS data assessment Life cycle Cost assessment Performance review		

A.4 List of techniques

Some appropriate methods and tools for conducting and managing RAMS activities 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. Procedures for formal design reviews with emphasis on RAMS, using some general and application specific check lists as appropriate, e.g.:

EN 61160:2005 Design review

2. 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

EN 60706-2 Part 2 - Maintainability requirements and studies during the design and development phase

EN 60706-3 Part 3 - Verification and collection, analysis and presentation of data

EN 60706-5 Part 5 - Testability and diagnostic testing

IEC 60706-6 Part 6 - Section 9: Statistical methods in maintainability evaluation

EN 60812 Analysis techniques for system reliability - Procedures for failure mode and effects analysis (FMEA)

EN 61025 Fault tree analysis (FTA)

EN 61078 Analysis techniques for dependability - Reliability block diagram and boolean methods

EN 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.:

EN 61709	Electronic components - Reliability - Reference conditions for failure rate and stress models for conversion
MIL-HDBK-217F Notice 2	Reliability Prediction for Electronic Systems

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

3. Procedures for performing hazard & safety/risk analysis

Some of these are described in:

MIL-STD-882D	Standard Practise for System Safety
MIL-HDBK-764 (MI)	System Safety Engineering Design Guide For Army Materiel

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", specifically the following parts:

EN 61508-5:2010	Part 5: Examples of methods for the determination of safety integrity levels
EN 61508-7:2010	Part 7: Overview of techniques and measures

4. RAMS testing plans and procedures

This step is 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 60605-2	Part 2: Design of test cycles
IEC 60605-3-1	Part 3: Preferred test conditions. Indoor portable equipment - Low degree of simulation
IEC 60605-4	Part 4: Statistical procedures for exponential distribution - Point estimates, confidence intervals, prediction intervals and tolerance intervals
IEC 60605-6	Part 6: Tests for the validity of the constant failure rate or constant failure intensity assumptions
EN 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.:

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

5. Procedures/tools to perform LCC analysis (Life cycle Cost)

Various computer programmes are available for LCC analysis.

Annex B
(informative)

Examples of parameters for railway

B.1 General

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

NOTE Some parameters in the examples are used only in specific sectors, e.g. rolling stock.

In general, any time-based parameter like MTBF can be converted/derived from the respective operated distance or operation cycles as well.

Definition and detailed guidance on mathematical treatment of RAM terms is given in EN 61703.

B.2 Reliability parameters

Table B.1 — Examples of reliability parameters

Parameter	Symbol	Dimension
Failure Rate	λ(t)	1/time, 1/distance, 1/cycle
Mean Up Time	MUT	time (distance, cycle)
Mean operating [a] Time To Failure (for non-repairable items)	MTTF	time (distance, cycle)
Mean operating [a]Time Between Failure (for repairable items)	MTBF	time (distance, cycle)
Failure Probability	F(t)	dimensionless
Reliability (Success Probability)	R(t)	dimensionless
[a] According to EN 61703 and IEC 60050-191-2.		

B.3 Maintainability parameters

Table B.2 — Examples of maintainability parameters

Parameter	Symbol	Dimension
Mean Down Time	MDT	time (distance, cycle)
Mean operating [a] Time Between Maintenance	MTBM	time (distance, cycles)
MTBM (corrective or preventive)	MTBM(c), MTBM(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
Mean Repair Time	MRT	time
Fault Coverage	FC	dimensionless
Repair Coverage	RC	dimensionless
[a] According to EN 61703 and IEC 60050-191-2.		

B.4 Availability parameters

Table B.3 — Examples of availability parameters

Parameter	Symbol	Dimension
Availability inherent operational	A A_i A_o	dimensionless
Fleet Availability	FA	dimensionless
Schedule Adherence	SA	dimensionless or time

Under certain conditions, for instance constant failure rate, constant repair rate and no preventative maintenance (MTTR=MDT), the steady-state availability can be expressed by

$$A = \frac{MUT}{MUT + MDT} \leq 1$$

with 0 ≤ A ≤ 1 and generally has a value close to 1. Its complement is called *unavailability U.*

$$U = 1 - A = \frac{MDT}{MUT + MDT} \geq 0$$

Depending on the type of availability A to be considered, it should be decided which fractions of MDT are relevant and therefore taken into consideration for calculation. These fractions are to be defined.

Detailed guidance on calculations for systems with different properties and different repair characteristics is given in EN 61703.

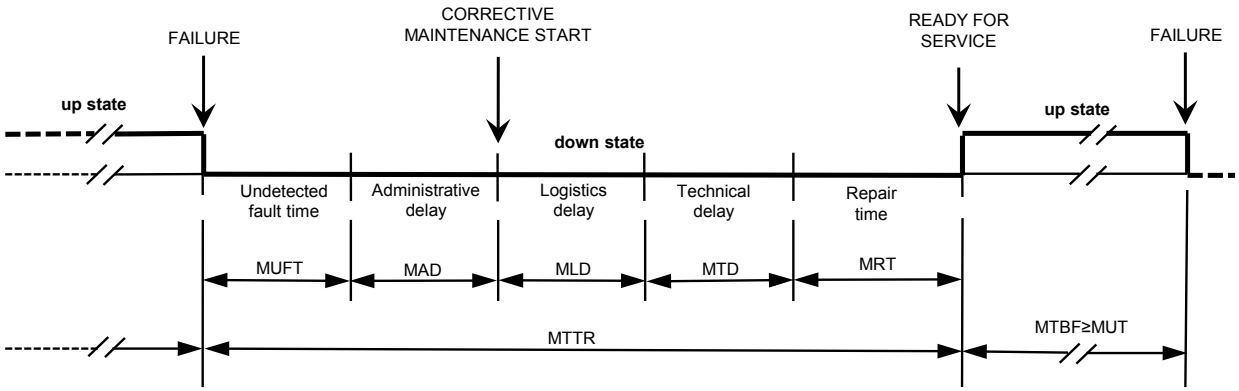
The availability concept is illustrated in Figure B.1.

For an item/system which is permanently in operation mode and no planned preventive maintenance is applied, MUT=MTTF holds. In this case MUT and MTTF can be used interchangeably for calculating the (steady state) operational availability. It can then be expressed by

$$A = \frac{MUT}{MUT + MDT} = \frac{MTTF}{MTTF + MTTR} \leq 1$$

MTBF is typically based on the time the system is in use (operated).

The parties involved should agree on the understanding of all the terms used (e.g. the MTBF time basis suitable for the specific application under consideration or which type of delay is taken into account). In case of contractual obligations, the agreements should be clearly stipulated.



Key

MTBF mean (operating) time between failures

MUT mean up time

MUFT mean undetected fault time

MAD mean administrative delay

MLD mean logistics delay

MTD mean technical delay

MRT mean repair time

MTTR mean time to restore (for corrective maintenance)

NOTE Definitions can be found in EN 61703.

Figure B.1 — Availability concept and related terms

NOTE 1 Detailed guidance on calculations with different system properties and different repair characteristics is given in EN 61703.

NOTE 2 Restoration can be achieved by repair, exchange, reset or other means.

The definitions of Fleet Availability (FA) as well as of Schedule Adherence (SA) are normally the subject of contractual negotiations. Therefore the elaboration of both parameters is not provided in this standard.

B.5 Logistic support parameters

Table B.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)
Mean Logistic Delay	MLD	time
Mean Administrative Delay	MAD	time
Fault correction time	-	time
Mean Repair Time	MRT	time
Turn Around Time	TAT	time
Maintenance support performance	-	dimensionless
Employees for Replacement	EFR	number
Probability that Spare Parts are available (in Stock) when needed	SPS	dimensionless

B.6 Safety parameters

Table B.5 — Examples of safety performance parameters

Parameter	Symbol	Dimension
Hazard rate	h(t)	1/time, 1/distance, 1/cycle
Probability of wrong-side failure	p_{WSF}	dimensionless
Active time to return to safe state	-	time

Annex C
(informative)

Risk matrix calibration and risk acceptance categories

C.1 General

Annex C provides examples of application of a risk matrix and its parameters.

- For the purpose of classifying any events, Table C.1 and Table C.2 provide, in qualitative terms, typical categories of probability or frequency of occurrence of events and a typical description of each category for railways. Based on these typical categories, their numbers, and their numerical scaling (provided that numerical estimates are feasible) to be applied shall be defined by the railway duty holder, appropriate to the application under consideration.

- Table C.3 to Table C.6 in Annex C describe typical severity categories and the associated consequences. The number of severity categories and the consequences for each severity category to be applied should be defined by the railway duty holder, appropriate for the application under consideration.

- With regard to safety, the relationship between injuries and fatalities ("equivalent fatalities" as defined in 3.19), for the purpose of predicting and comparison only, should be agreed with the railway duty holder based on the relevant legal framework.

- Examples of such relationship may be:

    - one equivalent fatality ≈ 1 fatality ≈ 10 major injuries ≈ 100 minor injuries or

    - severe injuries and fatalities are fully equivalent or

    - any other weighted equivalence.

C.2 Frequency of occurrence categories

The following Table C.1 and Table C.2 give examples of frequency categories, adapted to a particular use.

The use of these particular examples is not mandatory and other classifications may be used.

Table C.1 — Frequency of occurrence of hazardous events with examples for quantification (time based)

Frequency level	Description	Example of a frequency range based on a single item operating 24 h/day	Example of equivalent occurrence in a 30 year lifetime of a single item operating 5000 h/year
		Expected to happen	
Frequent	Likely to occur frequently. The event will be frequently experienced.	more than once within a period of approximately 6 weeks	more than about 150 times
Probable	Will occur several times. The event can be expected to occur often.	approximately once per 6 weeks to once per year	about 15 to 150 times
Occasional	Likely to occur several times. The event can be expected to occur several times.	approximately once per 1 year to once per 10 years	about 2 to 15 times
Rare	Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur.	approximately once per 10 years to once per 1 000 years	perhaps once at most
Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.	approximately once per 1 000 years to once per 100 000 years	not expected to happen within the lifetime
Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.	once in a period of approximately 100 000 years or more	extremely unlikely to happen within the lifetime

NOTE The examples given in this table relate to a single item (system/function/component) and can be adjusted dependent on the number of systems and/or the number of e.g. operational hours considered.

Where the frequency is constant, the expected mean time between two events is given by the reciprocal of the frequency. For a frequency level bandwidth this formula should be applied for its upper as well as its lower limit.

EXAMPLE 1: For a rate of 10^{-4} h^{-1}:

$1/10^{-4}$ h^{-1} = 10 000 h which means an expected event frequency of approximately:

- 1,2 years in case of 24 h operation
- or 2 years in case of assumed 5 000 h operating time per year.

The expected occurrence or number of events in a time period is determined by the given time period multiplied by the given rate or frequency of occurrence. The time period should be reduced if calendar time is not appropriate.

EXAMPLE 2: 10^{-4} h^{-1} x (30 years x 5 000 h/years) = 15 → The event is expected to happen approximately 15 times within 30 years if 5 000 operational hours per year are assumed. 10^{-4} h^{-1} x (30 years x 5 000 h/years) x 10 items = 150 → it is expected that approximately 150 failures will occur among the 10 items during the 30 years.

The considered time is an average and not necessarily a continuous time.

A distance based approach is given in Table C.2.

Table C.2 — Frequency of occurrence of events with examples for quantification (distance based)

Frequency level	Description	Example of a range of frequency
F1	Likely to occur often	more than once every 5 000 km per train
F2	Will occur several times	once every 25 000 km per train
F3	Might occur sometimes	once every 100 000 km per train

C.3 Severity categories

The following tables give examples of severity categories, related to a particular use.

Table C.3 — Severity categories (example related to RAM)

RAM severity category	Description
Significant (immobilising 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: • prevents the system from achieving its 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

Table C.4 — Severity categories (example 1 related to RAMS)

Severity category	Consequences to persons or environment	Consequences on service/property
Catastrophic	• Affecting a large number of people and resulting in multiple fatalities, and/or • extreme damage to the environment	Any of the below consequences in presence of consequences to persons or environment
Critical	• Affecting a very small number of people and resulting in at least one fatality, and/or • large damage to the environment	Loss of a major system
Marginal	• No possibility of fatality, severe or minor injuries only, and/or • minor damage to the environment	Severe system(s) damage
Insignificant	• Possible minor injury	Minor system damage

Table C.5 — Severity categories (example 2 related to Safety)

Severity category	Consequences to persons or environment
S1	Many equivalent fatalities (likely more than about 10) or extreme damage to the environment.
S2	Multiple equivalent fatalities (likely less than about 10) or large damage to the environment.
S3	Single fatality or severe injury or significant damage to the environment.
S4	Minor injuries or minor damage to the environment
S5	Possible minor injury

Table C.6 — Financial severity categories (example)

Severity category	Financial consequences
SF1	The incident will incur people suing the company, severe impact to the public image of the company, and/or incur costs higher than 1 000 000 €.
SF2	The incident may have an impact on the public image of the company and/or incur costs higher than 100 000 €
SF3	The incident will not incur costs higher than 100 000 €

C.4 Risk acceptance categories

Risk acceptance categories allocated to identified risks allow classification for the purpose of decision making. The choice of which risk acceptance categories to use should depend on the choice of risk acceptance criteria chosen and the decision to be made. Examples of risk acceptance categories are shown in Table C.7 and Table C.8 below:

Table C.7 — Risk acceptance categories (example 1 for binary decisions)

Risk Acceptance Category	Actions to be applied
Unacceptable	The risk needs further reduction to be accepted
Acceptable	The risk is accepted provided adequate control is maintained

Table C.8 — Risk acceptance categories (example 2)

Risk Acceptance Category	Actions to be applied
Intolerable	The risk shall be eliminated
Undesirable	The risk shall only be accepted if its reduction is impracticable and with the agreement of the railway duty holders or the responsible Safety Regulatory Authority.
Tolerable	The risk can be tolerated and accepted with adequate control (e.g. maintenance procedures or rules) and with the agreement of the responsible railway duty holders.
Negligible	The risk is acceptable without the agreement of the railway duty holders.

Risk matrix calibration should be performed based on the risk acceptance criteria, the frequency of occurrence categories and the severity categories. An example of a calibrated risk matrix is shown in Table C.9.

Table C.9 — Risk acceptance categories (example related to safety)

Frequency of occurrence of an accident (caused by a hazard)	Risk Acceptance Categories			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Rare	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Undesirable
Highly improbable	Negligible	Negligible	Negligible	Tolerable
	Insignificant	Marginal	Critical	Catastrophic
	Severity of an accident (caused by a hazard)			

Risk Acceptance Criteria can be also defined, either by railway duty holders or by legal requirements, directly in terms of the Tolerable Hazard Rates (THR). The THR is determined by the severity of the consequences resulting from the hazard.

EXAMPLE A reference quantitative safety target (THR) for Risk Acceptance Criteria based on Explicit Risk Estimation could be defined as: For technical systems where a failure has a credible potential to lead directly to a catastrophic accident, the associated risk does not need to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable. Where a functional failure has a credible direct potential for a catastrophic consequence, the associated risk does not need to be reduced further if the rate of that failure is less than or equal to 1×10^{-9} per operating hour.

The quantitative safety target expressed as THR for a given hazard should relate to specific elementary functions without considering its number of instances in whole railway system. This will avoid that a given technical system fulfilling a defined THR and already accepted in a specific application, would no longer be considered accepted when used in a different application.

Annex D
(informative)

Guidance on system definition

D.1 General

Annex D provides guidance on system definition.

D.2 System Definition in an iterative system approach

The risk assessment process is based on a system definition. The necessary activities and deliverables in the system definition phase are listed in 7.3.

An iterative method, as applicable for hierarchical systems, is used for defining a system and its subsystems. The iterative method is applicable in different phases of the life cycle. This could be in early phases of the functional breakdown of a system considering the safety aspects or in later phases where the method is applicable to the breakdown of functions or requirements, for example the allocation of functions to subsystems.

- The detailed procedures for system definition depend on the phase of the life cycle or the iterative level of the (sub-) system under consideration.

D.3 Method for defining the structure of a system

D.3.1 General

There are several types of breakdown structures, for example system breakdown structure or functional breakdown structure. For RAMS purposes the focus is on a functional breakdown which groups the functions together in a way that they can be carried out by a subsystem/product. In this case the functions of the system under consideration (including behaviour following failures, when defined) should be identified and described when the system definition is started.

D.3.2 Function List

A list of functions to be performed by the system under consideration should be identified and described when the system definition is started. It can be a preliminary list of functions and/or a preliminary system requirements specification depending on the level of application and on the level of known details of the functions.

D.3.3 Functional breakdown

The identified functions should be grouped together on the basis of:

– contribution to the same function of higher level;

– identified technical constraints (like subsystems/products to be reused).

Major external factors of the system should be also considered, including:

– the parties/stakeholders and boundaries of the system;

– physical and functional interfaces;

– limits of risk assessment.

Typical examples of the system functional breakdowns in the railway context are given below including subsystems that carry out the function.

Table D.1 — Typical examples for a functional breakdown

System	Functional breakdown group	Function	(Subsystem that carries out the function)
Fixed installations	Provide traction energy for trains	Convert, distribute and control electric energy	Substation & switching stations
		Transmit electric current to vehicle	Contact line systems
	Manage access to track	Open platform screen doors when train is present in station	Platform screen door system
	Control access to station	Allow full free passage in case of evacuation	Access gate system
Rolling stock	Control speed of train	Decelerate train	Brake system
		Hold train in standstill during stop	Brake system
	Control access to train	Hold all exits closed when vehicle is moving	Door control system
Control command and Signalling	Route control	Hold position of pointwork	Interlocking
		Indication signal aspect to driver	Interlocking
	Supervise speed of train	Ensure that train does not exceed maximum speed	Train control

D.4 Parties/stakeholders/boundaries of systems

When defining and analysing the system, consideration should be given to the system interfaces and boundaries of organisational responsibility. A failure that occurs in a system may propagate through its interfaces and have implications which can only be controlled by another organisation. In such cases the findings should be communicated to the other organisation in a timely manner.

D.5 Guidance on the content of a system definition

Clause 7.3.2 defines the aspects to be outlined for the content of system definition, including:

a) system and its mission profile;

b) system boundary. Examples of interactions with system boundary include:

– influence on neighbouring objects, systems, and environment including operational personnel, passengers, and public;

– definitions of physical and operational conditions and the environment under which the system works;

– description of necessary operator actions. Also identifying persons that are permitted to carry out these actions, indicating the skills and qualifications required and the basis for these actions, if any.

– In case of no human activities included in the description, provide the reasons for it.

c) Operational requirements. Examples of modes of operation include;

– normal, abnormal/degraded mode of operation, disconnect/connect states and transitions, etc., and their interactions;

– operational scenarios to be considered within the analysis, e.g. effects of maintenance operations (how, how often and by whom is the system maintained?).

– external requirements, e.g. external safety requirements resulting from the overall safety policy of the railway duty holder, from prevailing legal considerations, or from standards.

Annex ZZ
(informative)

Relationship between this European Standard and the Essential Requirements of EU Directive 2008/57/EC

This European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and within its scope the standard covers all relevant essential requirements as given in Annex III of the EC Directive 2008/57/EC (also named as New Approach Directive 2008/57/EC Rail Systems: Interoperability).

Once this standard is cited in the Official Journal of the European Union under that Directive and has been implemented as a national standard in at least one Member State, compliance with the clauses of this standard given in Table ZZ.1 for "Control-Command and Signalling", Table ZZ.2 "Locomotives and Passenger Rolling Stock", Table ZZ.3 for "Energy", Table ZZ.4 for "Infrastructure" confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding Essential Requirements of that Directive and associated EFTA regulations.

Table ZZ.1 — Correspondence between this European Standard, the TSI "Control-Command and Signalling" (COMMISSION REGULATION (EU) 2016/919 of 27 May 2016) and Directive 2008/57/EC

Clauses of this European Standard	Chapter/§/points/ of CCS TSI	Essential Requirements (ER) of Directive 2008/57/EC	Comments
	3.2. Specific Aspects of the Control-Command and Signalling Subsystems 3.2.1. Safety 3.2.2. Reliability and Availability	1. General Requirements 1.1 Safety 1.1.1 1.1.3 1.2. Reliability and availability	Reference to the standard in the TSI (Table A 3) and its Application Guide should be updated

Clauses of this European Standard	Chapter/§/points/ of CCS TSI	Essential Requirements (ER) of Directive 2008/57/EC	Comments
The whole standard is applicable. (To be applied together with EN 50126-2)	4.2. Functional and technical specifications of the Subsystems 4.2.1. Control-Command and Signalling safety characteristics relevant to interoperability 4.2.1.1. Safety 4.2.1.2. Availability/Reliability 4.5. Maintenance rules 4.5.1. Responsibility of the manufacturer of equipment 4.5.2. Responsibility of the applicant for subsystem verification 6. Assessing the conformity and/or suitability for use of the constituents and verifying the subsystems 6.2. Interoperability constituents 6.2.1. Assessment procedures for Control-Command and Signalling Interoperability Constituents 6.3. Control-Command and Signalling Subsystems	2. Requirements specific to each sub-subsystem 2.3. Control-command and signalling 2.3.1. Safety	

Table ZZ.2 — Correspondence between this European Standard, the TSI "Locomotives and Passenger Rolling Stock" (REGULATION (EU) No 1302/2014 of 18 November 2014) and Directive 2008/57/EC

Clauses of this European Standard	Chapter/§/points/ of LOC & PAS RST TSI	Essential Requirements (ER) of Directive 2008/57/EC	Comments
The whole standard is applicable. (To be applied together with EN is still applicable -2)	4.2. Functional and technical specification of the sub-system 6.2.3.5. Conformity assessment for safety requirements	1. General Requirements 1.1 Safety 1.1.1 1.1.3 1.2. Reliability and availability 2. Requirements specific to each sub-subsystem 2.4. Rolling Stock 2.4.1 Safety 2.4.2. Reliability and availability	Reference to the standard in the TSI Application Guide should be updated Only elements having requirements related to safety and/or reliability-availability as stated in clause 3 of the TSI.

Table ZZ.3 — Correspondence between this European Standard, the TSI "Energy" (REGULATION (EU) No 1301/2014 of 18 November 2014) and Directive 2008/57/EC

Clauses of this European Standard	Chapter/§/points/ of ENE TSI	Essential Requirements (ER) of Directive 2008/57/EC	Comments
The whole standard is applicable. (To be applied together with EN 50126-2)	4.4. Operating rules 4.5. Maintenance rules 4.6. Professional qualifications 4.7. Health and safety conditions	1. General Requirements 1.1 Safety 1.1.1 1.1.3 1.2. Reliability and availability 2. Requirements specific to each sub-subsystem 2.2 Energy 2.2.1 Safety	

Table ZZ.4 — Correspondence between this European Standard, the TSI "Infrastructure" (REGULATION (EU) No 1299/2014 of 18 November 2014) and Directive 2008/57/EC

Clauses of this European Standard	Chapter/§/points/ of INF TSI	Essential Requirements (ER) of Directive 2008/57/EC	Comments
The whole standard is applicable. (To be applied together with EN 50126-2)	2.5. Relation to the safety management system 4.4. Operating rules 4.5. Maintenance rules 4.6. Professional qualifications 4.7. Health and safety conditions	1. General Requirements 1.1 Safety 1.1.1 1.1.3 1.2. Reliability and availability 2. Requirements specific to each sub-subsystem 2.1. Infrastructure 2.1.1. Safety	

WARNING: Other requirements and other EU Directives may be applicable to the products falling within the scope of this standard.

Bibliography

EN 614	Safety of machinery — Ergonomic design principles
EN 60300-3-1	Dependability management — Part 3-1: Application guide — Analysis techniques for dependability — Guide on methodology (IEC 60300-3-1)
EN 60300-3-2	Dependability management — Part 3-2: Application guide — Collection of dependability data from the field (IEC 60300-3-2)
IEC 60319	Presentation and specification of reliability data for electronic components
IEC 60605-2	Equipment reliability testing — Part 2: Design of test cycles
IEC 60605-3-1	Equipment reliability testing — Part 3: Preferred test conditions. Indoor portable equipment — Low degree of simulation
IEC 60605-4	Equipment reliability testing — Part 4: Statistical procedures for exponential distribution — Point estimates, confidence intervals, prediction intervals and tolerance intervals
IEC 60605-6	Equipment reliability testing — Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity
IEC 60706-1	Guide on maintainability of equipment — Part 1: Sections 1, 2 and 3: Introduction, requirements and maintainability programme
EN 60706-2	Maintainability of equipment — Part 2: Maintainability requirements and studies during the design and development phase (IEC 60706-2)
EN 60706-3	Maintainability of equipment — Part 3: Verification and collection, analysis and presentation of data (IEC 60706-3)
EN 60706-5	Maintainability of equipment — Part 5: Testability and diagnostic testing (IEC 60706-5)
IEC 60706-6	Guide on maintainability of equipment — Part 6: Section 9: Statistical methods in maintainability evaluation
EN 60812	Analysis techniques for system reliability — Procedures for failure mode and effects analysis (FMEA) (IEC 60812)
EN 61014	Programmes for reliability growth (IEC 61014)
EN 61025	Fault tree analysis (FTA) (IEC 61025)
IEC 61070	Compliance test procedures for steady-state availability
EN 61078	Analysis techniques for dependability — Reliability block diagram and boolean methods (IEC 61078)
IEC 61123	Reliability testing — Compliance test plans for success ratio
EN 61160	Design review (IEC 61160)
EN 61165	Application of Markov techniques (IEC 61165)
EN 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems (IEC 61508)
EN 61703	Mathematical expressions for reliability, availability, maintainability and maintenance support terms (IEC 61703)
EN 61709	Electric components — Reliability — Reference conditions for failure rates and stress models for conversion (IEC 61709)
IEC/TR 62380	Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment
EN ISO 9001	Quality management systems — Requirements (ISO 9001)

ISO/IEC Guide 51	Safety aspects — Guidelines for their inclusion in standards
VDI 4006	Human reliability — Methods for event analysis regarding human behaviour

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.
- Standards purchased in hard copy format:
- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.