



BSI Standards Publication

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

Part 1: Generic RAMS process

National foreword

This British Standard is the UK implementation of EN 50126-1:2017+A1:2024. It supersedes BS EN 50126-1:2017, which will be withdrawn on 30 November 2027.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to CENELEC text carry the number of the CENELEC amendment. For example, text altered by CENELEC amendment A1 is indicated by A1 A1.

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 committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 14249 5

ICS 29.280; 45.020

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
30 November 2024	Implementation of CENELEC amendment A1:2024

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 FDMS 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

Contents

Page

European foreword	6
European foreword to Amendment 1	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	101
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.

European foreword to Amendment 1

This document (EN 50126-1:2017/A1:2024) has been prepared by Technical Committee 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) 2025-11-30
- latest date by which the national standards conflicting with this document have to be withdrawn (dow) 2027-11-30

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.

This document has been prepared under a standardization request addressed to CENELEC by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

For the relationship with EU Legislation, see informative Annex ZZ, which is an integral part of this document.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

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 **A1** the practical usage of this document **A1**, 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.

A1 The EN 50126 series **A1** 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.

A1 The EN 50126 series is independent from the technology used. As far as safety is concerned, the EN 50126 series takes the perspective of safety with a functional approach. **A1**

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

A1 This document **A1**

- 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 **A1** any former version of this document **A1**.

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

[A1] The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 50126-2:2017,¹ *Railway Applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Systems approach to safety* **[A1]**

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

[A1] unintended event or series of events that results in harm

[SOURCE: IEC 60050-821:2017, 821-12-02, modified – “that results in death, injury, loss of a system or service, or environmental damage” has been replaced with “that results in harm”] **[A1]**

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

[A1] 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: IEC 60050-902:2013, 902-03-04, modified – The Note 1 to entry has been omitted] **[A1]**

3.6

[A1] availability

<for railway RAMS> 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 60050-821:2017, 821-05-82, modified – “of a product” has been changed with “for railway RAMS”] **[A1]**

[A1] ¹ As impacted by EN 50126-2:2017/A1:2024. **[A1]**

3.7

basic integrity

A1 integrity attribute for a safety-related function with a TFFR equal to, or higher than (less demanding), 10^{-5} h^{-1} ; or for a non-safety-related function **A1**

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

A1 common cause failures

pl

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

Note 1 to entry: Common cause failures can also be “common mode failures”.

Note 2 to entry: The potential for common cause failures reduces the effectiveness of system redundancy.

[SOURCE: IEC 60050-192:2015; 192-03-18] **A1**

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: **A1** IEC 60050-821:2017 **A1**, 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 60050-821:2017 ^{A1}, 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**^{A1} 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.

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

Note 4 to entry: Inability to perform a function during maintenance activities does not need to be considered.

[SOURCE: IEC 60050-821:2017, 821-11-19, modified – Notes 3 and 4 to entry have been added] ^{A1}

3.22

failure mode

manner in which failure occurs

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

3.23

failure rate

[A1] 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 $(t, t + \Delta t)$ 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 IEC 192-05-07.

[SOURCE: IEC 60050-821:2017, 821-12-21] **[A1]**

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: **[A1]** IEC 60050-821:2017 **[A1]**, 821-11-20]

3.25

[A1] 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. **[A1]**

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

[A1] product independent of applications, fulfilling predefined boundary conditions, interfaces and functionality

EXAMPLES point machines, axle counters, real-time operating systems, fail-safe computer platform without application software

[SOURCE: IEC 60050-821:2017, 821-01-57, modified – "(blackbox)" has been removed] **[A1]**

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 60050-821:2017 , 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 60050-821:2017 , 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 60050-821:2017 , 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

A1 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, modified – The Note 2 to entry has been omitted.] A1

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: A1 IEC 60050-821:2017 A1, 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: A1 IEC 60050-821:2017 A1, 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 60050-821:2017 , 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**

 failure that occurs randomly in time

[SOURCE: IEC 60050-821:2017, 821-11-38] 

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

^{A1} risk

<for railway RAMS> combination of frequency of loss and the degree of severity of that loss

Note 1 to entry: In this document, risk is a general concept applicable both to safety and RAM aspects, i.e.:

- for safety, concerned losses involve harm;
- for RAM, concerned losses involve impact on operational capability, passenger's comfort or maintenance. ^{A1}

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 60050-821:2017 , 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 60050-821:2017 , 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 60050-821:2017 , 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

A1 ability of a safety-related function to perform satisfactorily with respect to safety under all the stated conditions within a stated operational environment and a stated period of time

[SOURCE: IEC 60050-821:2017, 821-12-54, modified – “system to achieve its required safety functions” has been replaced with “function to perform satisfactorily with respect to safety”; “within a stated duration” has been replaced with “a stated period of time”.] **A1**

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: **A1** IEC 60050-821:2017 **A1**, 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: **A1** IEC 60050-821:2017 **A1**, 821-01-73, note 1 to entry added]

3.75

safety-related application conditions

A1 those conditions which need to be met in order for a system to be safely integrated and safely operated

EXAMPLES operational conditions (e.g. speed limit, maximum duration of use, operational rules), maintenance conditions (e.g. requested maintenance intervals and rules) or environmental conditions. **A1**

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]

A1 3.84

harm

injury or damage to the health of people, or damage to property or the environment

[SOURCE: ISO/IEC Guide 51:2014, 3.1] **A1**

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.

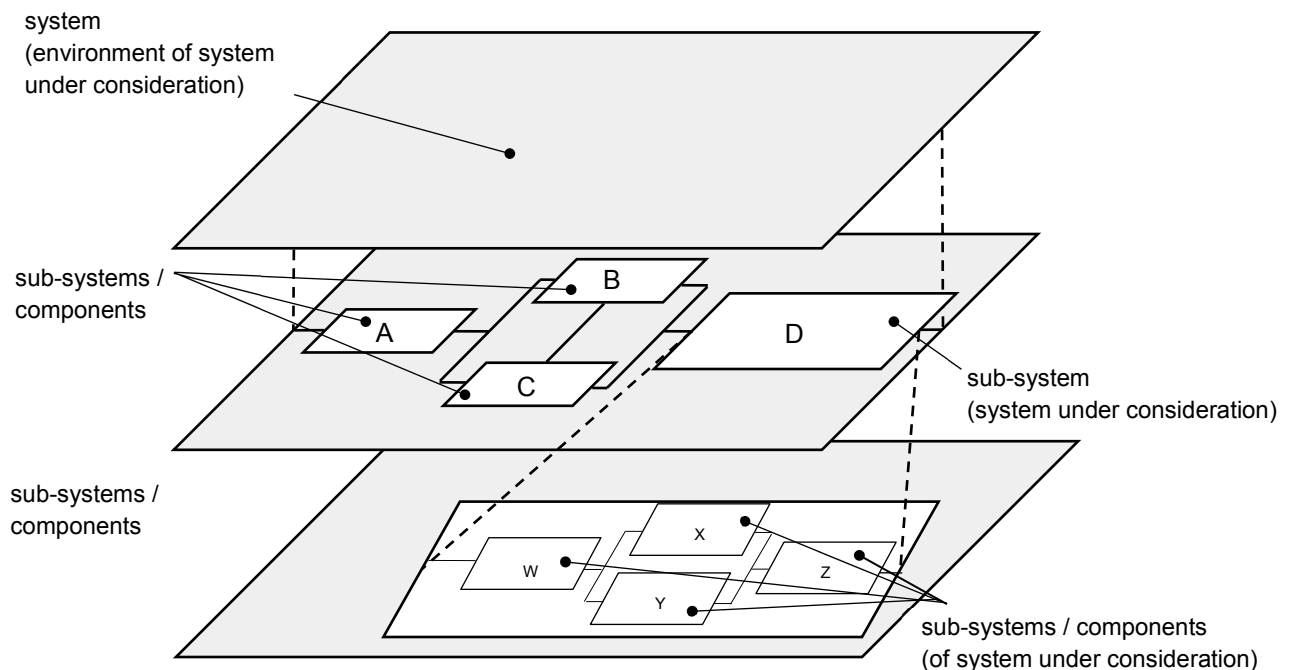


Figure 1 — Illustration of system hierarchy

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.

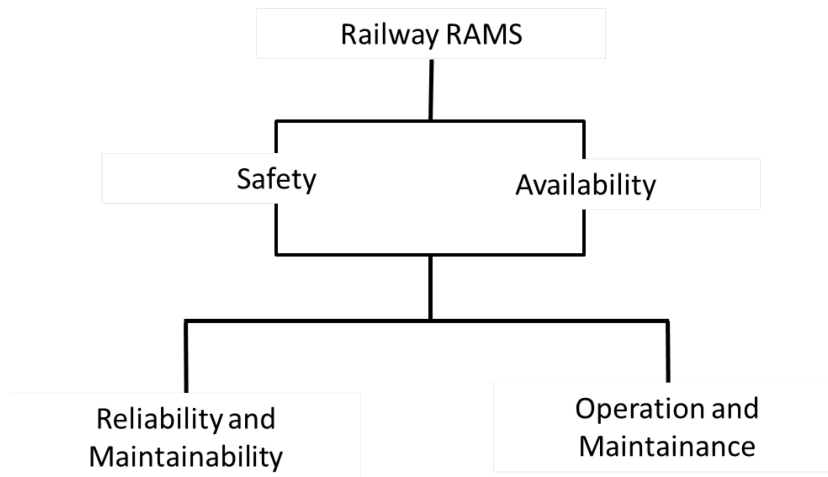


Figure 2 — Interrelation of railway RAMS elements

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.

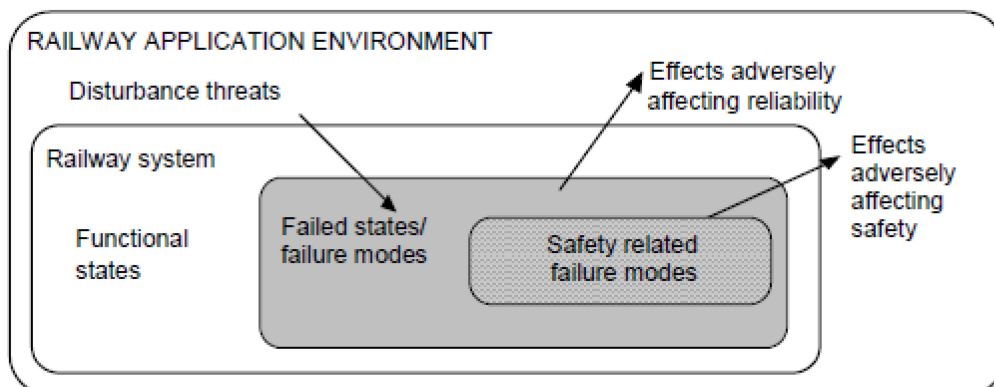


Figure 3 — Effects of failures within a system

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.

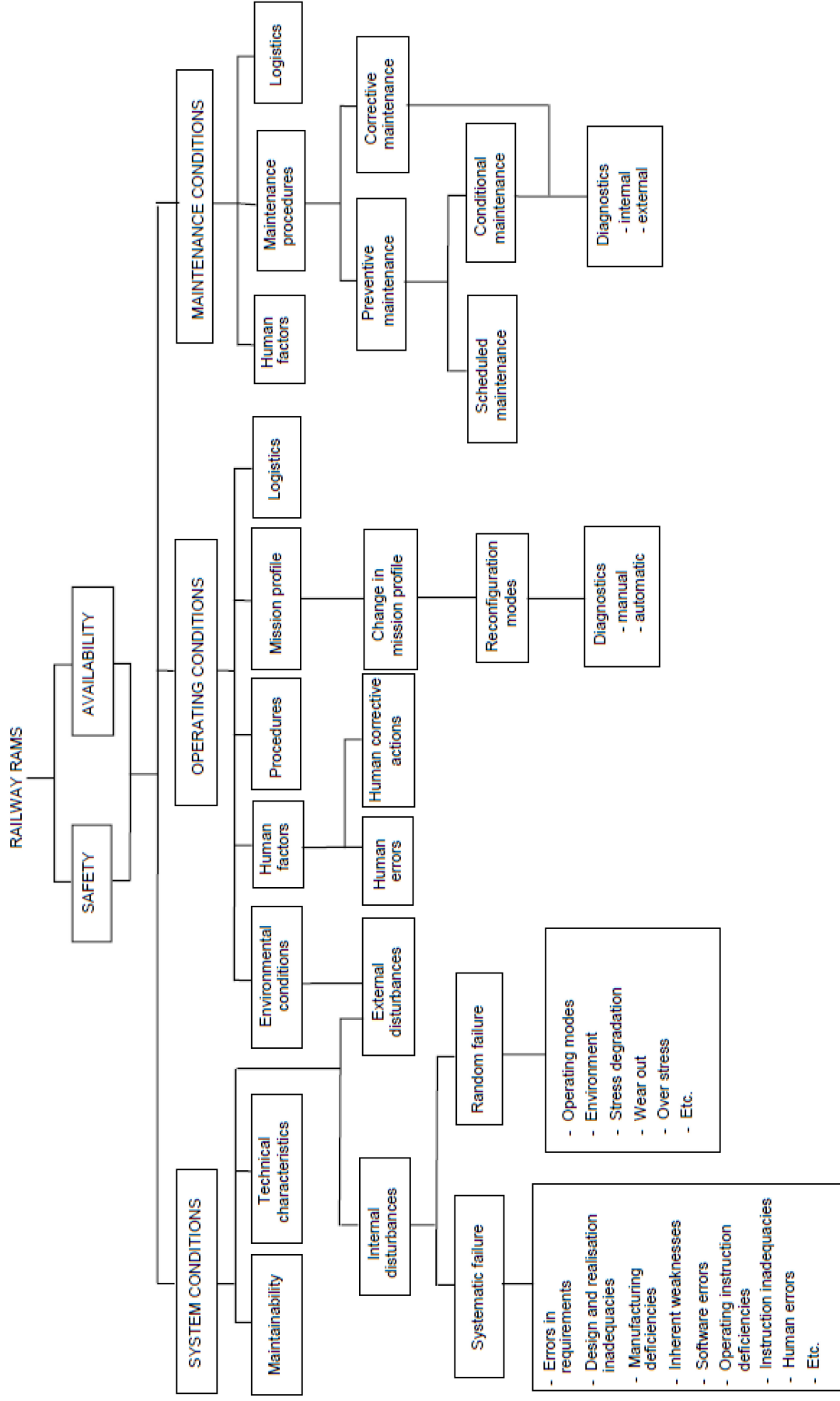


Figure 4 — Factors Influencing Railway RAMS

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