

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) -
Part 2: Systems approach to safety**

**Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) -
Partie 2: Approche systématique pour la sécurité**



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2025 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search -

webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication, or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées et retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Warning! Make sure that you obtained this publication from an authorized distributor.

Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD	5
INTRODUCTION	7
1 Scope	8
2 Normative references	9
3 Terms and definitions	9
4 Abbreviated terms	9
5 Safety process	10
5.1 Hourglass model for risk assessment and hazard control.....	10
5.2 A. Risk assessment.....	11
5.2.1 General.....	11
5.2.2 Conducting risk assessment.....	12
5.3 B. Outcome of the risk assessment.....	12
5.4 C. Hazard control	12
5.5 D. Revision of risk assessment.....	13
5.6 Responsibilities	14
6 Safety demonstration and acceptance.....	14
6.1 General	14
6.2 Safety demonstration and safety acceptance process	14
6.3 Responsibility in managing the safety case	18
6.4 Modifications after safety acceptance	18
6.5 Dependencies between safety cases	18
6.6 Relationship between safety cases and system architecture.....	19
7 Organization and independence of roles	20
7.1 General	20
7.2 Early phases of the life cycle (phases 1 to 4).....	21
7.3 Later phases of the life cycle (starting from phase 5).....	21
7.4 Personnel competence	23
8 Risk assessment.....	24
8.1 General	24
8.2 Risk analysis	24
8.2.1 General.....	24
8.2.2 The risk model	24
8.2.3 Techniques for the consequence analysis	26
8.2.4 Expert judgement.....	27
8.3 Risk acceptance principles and risk evaluation	28
8.3.1 Use of code of practice	28
8.3.2 Use of a reference system.....	28
8.3.3 Use of explicit risk estimation	29
8.4 Application of explicit risk estimation	30
8.4.1 Quantitative approach	30
8.4.2 Variability using quantitative risk estimates	33
8.4.3 Qualitative and semi-quantitative approaches	34
9 Specification of system safety requirements.....	35
9.1 General	35
9.2 Safety requirements	35

9.3	Categorization of safety requirements	35
9.3.1	General	35
9.3.2	Functional safety requirements	36
9.3.3	Technical safety requirements	37
9.3.4	Contextual safety requirements	37
10	Apportionment of functional safety integrity requirements	38
10.1	General	38
10.2	Functional safety integrity for electronic systems	38
10.2.1	General	38
10.2.2	Apportioning safety requirements	38
10.2.3	Safety integrity factors	41
10.2.4	Functional safety integrity and random failures	41
10.2.5	Systematic aspect of functional safety integrity	41
10.2.6	Balanced requirements controlling random and systematic failures	42
10.2.7	The SIL table	42
10.2.8	SIL allocation	43
10.2.9	Apportionment of TFFR after SIL allocation	43
10.2.10	Demonstration of quantified targets	44
10.2.11	Requirements for basic integrity	44
10.2.12	Prevention of misuse of SILs	45
10.3	Safety integrity for non-electronic systems - Application of CoP	45
11	Design and implementation	46
11.1	General	46
11.2	Causal analysis	46
11.3	Hazard identification (refinement)	47
11.4	Common cause failure analysis	48
Annex A (informative)	ALARP, GAME, MEM as examples of risk acceptance criteria	50
A.1	ALARP, GAME, MEM as methods to define risk acceptance criteria	50
A.2	ALARP (as low as reasonably practicable)	51
A.2.1	General	51
A.2.2	Tolerability and ALARP	51
A.3	Globalement au moins équivalent (GAME) principle	52
A.3.1	Principle	52
A.3.2	Using GAME	52
A.4	Minimum endogenous mortality (MEM)	53
Annex B (informative)	Using failure and accident statistics to derive a THR	56
Annex C (informative)	Guidance on SIL allocation	58
Annex D (informative)	Safety target apportionment methods	59
D.1	Analysis of the system and methods	59
D.2	Example of qualitative apportionment method	59
D.2.1	General	59
D.2.2	Example of qualitative or semi-quantitative method for barrier efficiency	60
D.3	Example of quantitative apportionment method	62
D.3.1	General	62
D.3.2	Functions with independent failure detection and negation mechanisms	64
D.3.3	Function and independent barrier acting as failure detection and negation mechanism	65

D.3.4	Apportionment of a probability safety target	67
D.3.5	Apportionment of a "per hour" safety target	67
Annex E (informative)	Common mistakes in quantification	69
E.1	General	69
E.2	Mixing failure rates with probabilities	69
E.3	Using formulas out of their range of applicability	70
Annex F (informative)	Techniques and methods for safety analysis	71
Annex G (informative)	Key system safety roles and responsibilities	73
Bibliography	78
Figure 1	– The hourglass model	11
Figure 2	– Illustration of hazards with respect to the system boundary	11
Figure 3	– Example of safety acceptance processes	17
Figure 4	– Examples of dependencies between safety cases	19
Figure 5	– Independence of roles in the early phases (phases 1 to 4) of the life cycle	21
Figure 6	– Independence of roles in later phases of the life cycle (starting from phase 5)	23
Figure 7	– An example of risk model	25
Figure 8	– Tolerable rates in an example of risk model	31
Figure 9	– Requirements classification	36
Figure 10	– Apportionment of functional safety requirements	39
Figure 11	– Categorization of safety integrity measures	42
Figure 12	– Common cause failures	48
Figure 13	– Impact of functional dependence in a fault tree analysis	48
Figure A.1	– Differential risk aversion	54
Figure D.1	– Example of qualitative apportionment method	60
Figure D.2	– Interpretation of failure and repair times	63
Figure D.3	– Combination of two functions with independent failure detection and negation mechanism	64
Figure D.4	– Allocation of safety integrity requirements	65
Figure D.5	– Combination of function and independent barrier acting as failure detection and negation mechanism	66
Figure D.6	– Example of quantified apportionment	68
Figure E.1	– Example of TIA case	69
Table 1	– Examples of hazards	26
Table 2	– SIL quantitative and qualitative measures	43
Table D.1	– Overview of ALARP, GAME, MEM	50
Table D.1	– Efficiency based on the component's failures	61
Table D.2	– Efficiency based on the component's knowledge	61
Table D.3	– Efficiency based on the use of the component	61
Table D.4	– Efficiency based on the maintenance of the component	62
Table F.1	– Techniques and methods for safety analysis	71
Table F.2	– Techniques and measures for BI and SILs	72

Table G.1 – Role specification for designer	73
Table G.2 – Role specification for verifier	74
Table G.3 – Role specification for validator	75
Table G.4 – Role specification for independent safety assessor	76
Table G.5 – Role specification for project manager.....	77

Currently in preview, click buy full version

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**Railway applications -
Specification and demonstration of reliability, availability, maintainability
and safety (RAMS) -
Part 2: Systems approach to safety**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch> shall not be held responsible for identifying any or all such patent rights.

IEC 62278-2 has been prepared by IEC technical committee 9: Electric systems and equipment for railways. It is an International Standard.

This first edition, together with IEC 62278-1, cancels and replaces IEC 62278:2002. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) creation of this new Part 2 providing, for the first time, safety-related guidance and methods that support the safety management process provided in IEC 62278-1:2025.

The text of this International Standard is based on the following documents:

Draft	Report on voting
9/3208/FDIS	9/3235/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

The IEC 62278 series forms part of the railway sector specific application of IEC 61508. IEC 62278, IEC 62279 and IEC 62425 comprise the railway sector equivalent of the IEC 61508 series so far as railway communication, signalling and processing systems are concerned. When compliance with these documents has been demonstrated, further evaluation of compliance with the IEC 61508 series is not foreseen.

A list of all parts in the IEC 62278 series, published under the general title *Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under www.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

INTRODUCTION

IEC 62278:2002 was aimed at introducing the application of a systematic RAMS management process in the railway sector. Through the application of IEC 62278:2002 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 including signalling, rolling stock and fixed installations.

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

The IEC 62278 series is derived from the European Standard series EN 50126:2017, consisting of EN 50126-1:2017 and EN 50126-2:2017.

With regard to safety, IEC 62278-1 provides a safety management process which is supported by guidance and methods described in this document.

IEC 62278-1 and IEC 62278-2 are independent from the technology used. As far as safety is concerned, IEC 62278 takes the perspective of safety with a functional approach.

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

This document 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 document facilitates assessment of the RAMS interactions between elements of railway applications even if they are of complex nature.

This document promotes co-operation between the stakeholders of railways in the achievement of an optimal combination of RAMS and cost for railway applications.

The process defined by this document assumes that railway duty holders and railway suppliers have business-level policies addressing quality, performance and safety. The approach defined in this document is consistent with the application of quality management requirements contained within ISO 9001.

1 Scope

This document considers the safety-related generic aspects of the RAMS life cycle and defines methods and tools which are independent of the actual technology of the systems and subsystems.

This document provides:

- a) methods for the understanding of the systems approach to safety which is a key concept of IEC 62278;
- b) methods to derive the safety requirements and their safety integrity requirements for the system and to apportion them to the subsystems;
- c) methods to derive the safety integrity levels (SIL) for the safety-related electronic functions;
- d) guidance and methods for the following areas:
 - 1) safety process;
 - 2) safety demonstration and acceptance;
 - 3) organization and independence of roles;
 - 4) risk assessment;
 - 5) specification of safety requirements;
 - 6) apportionment of functional safety requirements;
 - 7) design and implementation;
- e) the user of this document with the methods to assure safety with respect to the system under consideration and its interactions;
- f) guidance about the definition of the system under consideration, including identification of the interfaces and the interactions of this system with its subsystems or other systems, in order to conduct the risk analysis.

This document does not specify:

- g) RAMS targets, quantities, requirements or solutions for specific railway applications;
- h) rules or processes pertaining to the certification of railway products against the requirements of this document;
- i) an approval process by the safety authority.

This document is applicable:

- j) 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:
 - 1) to new systems;
 - 2) 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;
 - 3) 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;
- k) at all relevant phases of the life cycle of an application;
- l) for use by railway duty holders and the railway suppliers.

This document is not applicable to:

- m) any unmodified aspect of the existing system;

- n) existing systems which remain unmodified, including those systems already compliant with IEC 62278:2002.

2 Normative references

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.

IEC 62278-1:2025, *Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1: Generic RAMS process*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62278-1 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

4 Abbreviated terms

ALARP	as low as reasonably practicable
CBA	cost benefit analysis
CCF	common cause failure analysis
CoP	code of practice
DRA	differential risk aversion
ERE	explicit risk estimation
EMC	electromagnetic compatibility
ETA	event tree analysis
FMECA	failure mode, effects and criticality analysis
FTA	fault tree analysis
GA	generic application
GASC	generic application safety case
GP	generic product
GPSC	generic product safety case
GAME	globalement au moins équivalent (globally at least equivalent)
HAZOP	hazard and operability study
IM	infrastructure manager
LRU	line replaceable unit
MDT	mean down time
MEM	minimum endogenous mortality
RAMS	reliability, availability, maintainability and safety
RAP	risk acceptance principle
RBD	reliability block diagram