

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Railway applications - Communication, signalling and processing systems -
Safety related electronic systems for signalling**

**Applications ferroviaires - Systèmes de signalisation, de télécommunication et
de traitement - Systèmes électroniques de sécurité pour la signalisation**



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 It also gives information on projects, replaced and withdrawn publications.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 ou 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.....	6
INTRODUCTION.....	8
1 Scope.....	9
2 Normative references	10
3 Terms, definitions and abbreviated terms	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms.....	21
4 Overall framework of this document.....	22
5 Requirements for developing safety-related electronic systems	24
5.1 General.....	24
5.2 The quality management process.....	24
5.3 The safety management process.....	26
5.3.1 General	26
5.3.2 Guideline for structuring documentation.....	26
5.3.3 Safety life cycle	27
5.3.4 Safety organization.....	27
5.3.5 Safety plan	29
5.3.6 Hazard log.....	30
5.3.7 Safety requirements specification	30
5.3.8 System design for safety	30
5.3.9 Safety operation and maintenance plan	31
5.3.10 Safety verification	31
5.3.11 Safety validation	32
5.3.12 Safety qualification tests.....	33
5.3.13 Management of safety-related application conditions	34
5.3.14 Safety justification	35
5.3.15 Independent safety assessment.....	36
6 Requirements for elements following different life cycles	36
6.1 General.....	36
6.2 Use of pre-existing items	37
6.2.1 General	37
6.2.2 Requirements for use of complete pre-existing systems.....	38
6.2.3 Requirements for use of pre-existing equipment	38
6.3 Safety-related tools for electronic systems	39
6.4 Physical security and cybersecurity.....	40
7 The safety case: structure and content	41
7.1 The safety case structure	41
7.2 The technical safety report.....	43
7.3 Generic and specific safety cases	52
7.4 Provisions for the specific application safety case.....	52
7.5 Dependencies between safety cases	53
8 System safety acceptance and subsequent phases	54
8.1 System safety acceptance process	54
8.2 Operation, maintenance and performance monitoring	58
8.3 Modification and retrofit	58
8.4 Decommissioning and disposal	58

Annex A (normative) Safety integrity levels	59
A.1 General.....	59
A.2 Safety requirements.....	59
A.3 Safety integrity.....	60
A.4 Determination of safety integrity requirements	60
A.4.1 General	60
A.4.2 Risk assessment	62
A.4.3 Hazard control	64
A.4.4 Identification and treatment of new hazards arising from design	70
A.5 Allocation of SILs	71
A.5.1 General aspects	71
A.5.2 Relationship between SIL and associated TFFR	72
Annex B (normative) Management of faults for safety-related functions	74
B.1 General.....	74
B.2 General concepts.....	74
B.2.1 Detection and negation times.....	74
B.2.2 Composition of two independent items.....	75
B.3 Effects of faults	76
B.3.1 Effects of single faults	76
B.3.2 Independence of items.....	78
B.3.3 Detection of single faults	83
B.3.4 Action following detection (retention of safe state)	86
B.3.5 Effects of multiple faults	87
B.3.6 Defence against systematic faults.....	90
Annex C (normative) Identification of hardware component failure modes	91
C.1 General.....	91
C.2 General procedure	91
C.3 Procedure for integrated circuits	91
C.4 Procedure for components with inherent physical properties	92
C.5 General provisions concerning component failure modes	92
Annex D (informative) Example of THR/TFFR/FR apportionment and SIL allocation.....	110
Annex E (normative) Techniques and measures for the avoidance of systematic faults and the control of random and systematic faults	112
E.1 General.....	112
E.2 Tables of techniques and measures	114
Annex F (informative) Guidance on User Programmable Integrated Circuits.....	122
F.1 General.....	122
F.1.1 Purpose	122
F.1.2 Terminology and context.....	122
F.2 UPIC life cycle	123
F.2.1 General	123
F.2.2 Organization, roles, responsibilities and personnel competencies	125
F.2.3 UPIC Requirements	125
F.2.4 UPIC Architecture and Design	126
F.2.5 Logic Component Design	127
F.2.6 Logic Component Coding.....	127
F.2.7 Logic Component Verification	127
F.2.8 UPIC Physical Implementation.....	127

F.2.9	UPIC Integration	127
F.2.10	UPIC Validation	127
F.2.11	Requirements for use of pre-existing logic components	127
F.3	Detailed technical requirements for UPIC.....	127
F.3.1	Guidance on safety architecture	127
F.3.2	Protection against random faults – architectural principles.....	128
F.3.3	Protection against systematic faults – techniques and measures	128
Annex G (informative)	Changes in this document compared to IEC 62425:2007.....	137
Bibliography		140
Figure 1	– Scope of the main IEC and CENELEC railway application standards.....	10
Figure 2	– Structure of IEC 62425.....	23
Figure 3	– Example of system life cycle	25
Figure 4	– Example of design and validation portion of system life cycle.....	27
Figure 5	– Independence of roles for different SILs and BI, phases 5 to 10	29
Figure 6	– Structure of safety case	42
Figure 7	– Structure of technical safety report.....	44
Figure 8	– Examples of different usage of safety cases.....	54
Figure 9	– Examples of different safety acceptance processes	57
Figure A.1	– Safety requirements and safety integrity	59
Figure A.2	– The hourglass model	62
Figure A.3	– Definition of hazards with respect to the system boundary	64
Figure A.4	– Example of a hazard analysis process	66
Figure A.5	– Common cause failures (CCF)	68
Figure A.6	– Treatment of CCF by FTA	69
Figure A.7	– Relationship between SILs and techniques	72
Figure B.1	– Detection and negation times.....	74
Figure B.2	– Control of single and multiple faults	78
Figure B.3	– Influences affecting the independence of items	80
Figure B.4	– Detection and negation of single faults – composite fail-safety.....	86
Figure B.5	– Detection and negation of single faults – reactive fail-safety	87
Figure C.1	– Example of a 4-terminal resistor, using a hybrid thick layer technique.....	94
Figure D.1	– Example of THR/TFFR/FR breakdown and related SIL allocation.....	110
Figure F.1	– UPIC architecture.....	123
Figure F.2	– UPIC development context.....	123
Figure F.3	– Example of UPIC development life cycle	124
Figure F.4	– Example of UPIC development life cycle with pre-existing components	124
Figure F.5	– UPIC development techniques and measures	129
Table 1	– Example of SRAC template	35
Table 2	– Sections and contents of the technical safety report.....	44
Table A.1	– The SIL table	72
Table B.1	– Measures to detect faults in integrated circuits by means of periodic online testing	88

Table C.1 – Resistors	94
Table C.2 – Capacitors	95
Table C.3 – Electromagnetic components	96
Table C.4 – Diodes	99
Table C.5 – Transistors.....	100
Table C.6 – Controlled rectifiers.....	102
Table C.7 – Surge suppressors.....	103
Table C.8 – Opto-electronic components	104
Table C.9 – Filters	106
Table C.10 – Interconnection assemblies.....	107
Table C.11 – Fuses.....	108
Table C.12 – Switches and push/pull buttons.....	108
Table C.13 – Lamps.....	108
Table C.14 – Batteries	109
Table C.15 – Transducers and sensors (excluding those with internal electronic circuitry)	109
Table E.1 – Safety planning and quality assurance activities	114
Table E.2 – Safety requirements specification.....	115
Table E.3 – Safety organization	115
Table E.4 – Architecture of system, subsystem or equipment.....	116
Table E.5 – Design features.....	117
Table E.6 – Failure and hazard analysis methods	118
Table E.7 – Design and development of system, subsystem or equipment	119
Table E.8 – Safety verification and validation of the system, subsystem or equipment	120
Table E.9 – Application, operation and maintenance.....	121
Table F.1 – Example of documentation generated during each phase	125
Table F.2 – Simplified techniques and measures for protection against systematic failures	129
Table F.3 – Design and verification (including all activities before synthesis)	130
Table F.4 – Synthesis	130
Table F.5 – Placement, routing and layout generation.....	131
Table F.6 – Description of techniques for design.....	131
Table F.7 – Description of techniques for synthesis	134
Table F.8 – Description of techniques for placement, routing and layout generation.....	136
Table G.1 – Clauses and subclauses – correspondence with IEC 62425:2007	137
Table G.2 – Figures and tables – correspondence with IEC 62425:2007	139

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**RAILWAY APPLICATIONS –
COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS –
SAFETY RELATED ELECTRONIC SYSTEMS FOR SIGNALLING****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>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62425 has been prepared by IEC technical committee 9: Electrical equipment and systems for railways. It is an International Standard.

EN 50129:2018 has served as a basis for the development of this document.

This second edition cancels and replaces the first edition published in 2007. This edition constitutes a technical revision.

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

- a) a better alignment with the life cycle phases defined in IEC 62278-1 has been made;
- b) Clause 5 describes the requirements that apply to the development of safety-related electronic systems (until phase 9 of the life cycle);

- c) Clause 8 focuses on the requirements for safety acceptance and approval of safety-related electronic systems and subsequent phases;
- d) requirements and guidance have been added in Clause 6 on the following topics:
 - 1) reuse of pre-existing systems,
 - 2) safety-related tools,
 - 3) impact of cybersecurity threats on functional safety,
 - 4) specific application safety cases;
- e) requirements for the structure and content of the safety case are now defined in a dedicated Clause 7;
- f) Annex A has been updated for the specification and allocation of safety integrity requirements;
- g) the content of former Annex D has been merged with Annex B, and the content has been changed from informative to normative;
- h) the status of Annex E has been changed from informative to normative;
- i) an Annex F has been added as an informative annex on User Programmable Integrated Circuits.

A more detailed comparison of changes between IEC 62425:2007 and this document can be found in Annex G.

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

Draft	Report on voting
9/3113/FDIS	9/3141/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 committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This International Standard defines requirements for the development and acceptance of safety-related electronic systems in the railway signalling field.

Safety-related electronic systems for signalling include hardware and software aspects. To develop complete safety-related systems, both aspects need to be taken into account throughout the whole life cycle of the system. The requirements for the overall safety-related electronic system and for its hardware aspects are defined in this document. Other requirements are defined in associated IEC and CENELEC standards. For safety-related systems which include software, additional conditions are defined in IEC 62279:2015.

NOTE 1 IEC 62279:2015 is derived from the European Standard EN 50128:2011.

Additional requirements for safety-related communication are defined in IEC 62280:2014.

This document is the common base for safety acceptance and approval of electronic systems for railway signalling applications. The aim of railway authorities and railway industry is to develop railway systems based on common standards. The safety authorities having jurisdiction can apply this document to the relevant matters they choose. On this basis, cross-acceptance of safety approvals for sub-systems and equipment can be applied by the different national safety authorities.

Cross-acceptance is applicable to generic approval, not to specific applications.

This document is concerned with the evidence to be presented for the acceptance of safety-related systems. However, it specifies not only those life cycle activities which need to be completed before the acceptance stage, but also the additional planned activities to be carried out afterwards. In this way, safety justification will cover the whole life cycle.

This document is concerned with what evidence is to be presented. Except where considered appropriate, it does not specify who carries out the necessary work. The necessary work can be carried out by different people, in different circumstances or organisational structures, provided that independence of roles is respected.

This document consists of Clauses 1 to 8, which form the main part, and Annexes A, B, C, D, E, F and G. The requirements defined in Clauses 5 to 8 and in Annexes A, B, C and E are normative, whilst Annexes D, F and G are informative.

This document is in line with, and contain references to IEC 62278-1:—¹ and IEC 62278-2:—¹.

NOTE 2 IEC 62278-1:— and IEC 62278-2:— are derived from the European Standards EN 50126-1:2017 and EN 50126-2:2017 respectively.

This document is based on the system life cycle described in IEC 62278 series and is in line with the IEC 61508 series. 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. Given that compliance with these documents has been demonstrated, there are no requirements in this document for further evaluation of compliance with the IEC 61508 series.

¹ Under preparation. Stage at the time of publication: IEC/FDIS 62278-1:2025 and IEC/FDIS 62278-2:2025.

RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS – SAFETY RELATED ELECTRONIC SYSTEMS FOR SIGNALLING

1 Scope

This document is applicable to safety-related electronic systems (including subsystems and equipment) for railway signalling applications.

This document applies to generic systems (i.e. generic products or systems defining a class of applications), as well as to systems for specific applications.

The scope of this document, and its relationship with other IEC and CENELEC standards, are shown in Figure 1.

This document is applicable only to the functional safety of systems. It does not deal with other aspects of safety such as the occupational health and safety of personnel. While functional safety of systems clearly can have an impact on the safety of personnel, there are other aspects of system design which can also affect occupational health and safety and which are not covered by this document. Cybersecurity aspects of functional safety are addressed only to a limited extent.

This document applies to all the phases of the life cycle of a safety-related electronic system, focusing in particular on phases 5 (architecture and apportionment of system requirements) to 10 (system acceptance) as defined in IEC 62278-1:—.

Requirements for systems which are not related to safety are outside the scope of this document.

This document is not applicable to existing systems, subsystems or equipment which had already been accepted prior to the development of this document. However, so far as reasonably practicable, it is applicable to modifications and extensions to existing systems, subsystems and equipment.

This document is primarily applicable to systems, subsystems or equipment which have been specifically designed and manufactured for railway signalling applications. It is also applicable, so far as reasonably practicable, to general-purpose or industrial equipment (e.g. power supplies, display screens or other commercial off the shelf items), which is procured for use as part of a safety-related electronic system.

This document is aimed at railway duty holders, railway suppliers, and assessors as well as at safety authorities, although it does not define an approval process to be applied by the safety authorities.

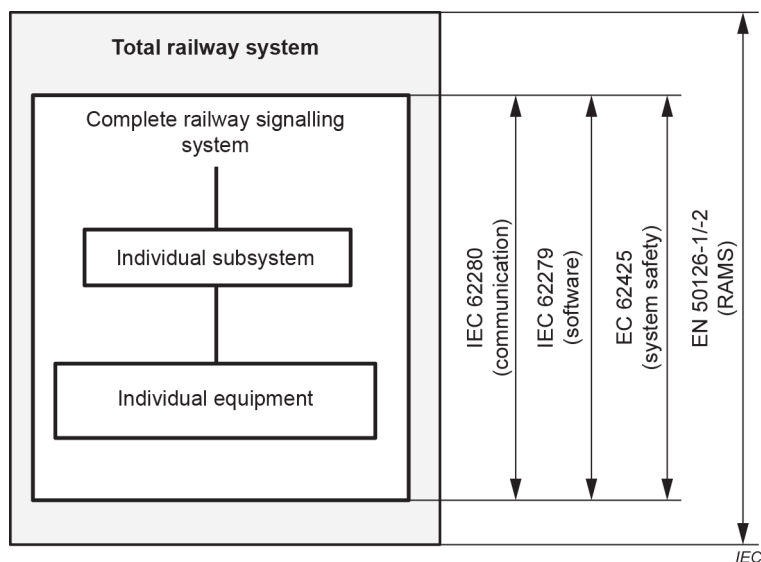


Figure 1 – Scope of the main IEC and CENELEC railway application standards

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 60664-1:2020, *Insulation coordination for equipment within low-voltage supply systems – Part 1: Principles, requirements and tests*

IEC 62278-1:—², *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process*

IEC 62278-2:—², *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety*

IEC 62279:2015, *Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems*

IEC 62280:2014, *Railway applications – Communication, signalling and processing systems – Safety related communication in transmission systems*

IEC 62497-1³:2010, *Railway applications – Insulation coordination – Part 1: Basic requirements – Clearances and creepage distances for all electrical and electronic equipment*
IEC 62497-1:2010/AMD1:2013

IEC 62498-1:2010, *Railway applications – Environmental conditions for equipment – Part 1: Equipment on board rolling stock*

IEC 62498-3:2010, *Railway applications – Environmental conditions for equipment – Part 3: Equipment for signalling and telecommunications*

² Under preparation. Stage at the time of publication: IEC/FDIS 62278-1:2025 and IEC/FDIS 62278-2:2025.

³ There exists a consolidated edition 1.1:2013 that includes IEC 62497-1:2010 and its Amendment 1:2013.

SOMMAIRE

AVANT-PROPOS	146
INTRODUCTION.....	148
1 Domaine d'application	150
2 Références normatives	151
3 Termes, définitions et abréviations	152
3.1 Termes et définitions	152
3.2 Termes abrégés	163
4 Structure générale du présent document	164
5 Exigences relatives au développement de systèmes électroniques relatifs à la sécurité	165
5.1 Généralités	165
5.2 Processus de gestion de la qualité	165
5.3 Processus de gestion de la sécurité	168
5.3.1 Généralités	168
5.3.2 Lignes directrices pour la structuration de la documentation	168
5.3.3 Cycle de vie sécurité	169
5.3.4 Organisation de la sécurité	169
5.3.5 Plan de sécurité	171
5.3.6 Registre des dangers	172
5.3.7 Spécification des exigences de sécurité	172
5.3.8 Conception du système pour la sécurité	172
5.3.9 Plan de maintenance et d'exploitation de sécurité	173
5.3.10 Vérification de la sécurité	173
5.3.11 Validation de la sécurité	174
5.3.12 Essais de qualification de sécurité	175
5.3.13 Gestion des conditions d'utilisation relatives à la sécurité	176
5.3.14 Justification de la sécurité	178
5.3.15 Évaluation indépendante de la sécurité	178
6 Exigences relatives aux éléments suivant différents cycles de vie	179
6.1 Généralités	179
6.2 Utilisation des entités préexistantes	179
6.2.1 Généralités	179
6.2.2 Exigences relatives à l'utilisation de systèmes préexistants complets	180
6.2.3 Exigences relatives à l'utilisation d'équipements préexistants	180
6.3 Outils relatifs à la sécurité pour les systèmes électroniques	181
6.4 Sécurité physique et cybersécurité	183
7 Dossier de sécurité : plan et contenu	184
7.1 Plan du dossier de sécurité	184
7.2 Le rapport de sécurité technique	186
7.3 Dossiers de sécurité génériques et spécifiques	195
7.4 Dispositions relatives au dossier de sécurité pour une application spécifique (SASC)	196
7.5 Dépendances entre les dossiers de sécurité	197
8 Acceptation de la sécurité du système et phases suivantes	198
8.1 Processus d'acceptation de la sécurité du système	198
8.2 Suivi de l'exploitation, de la maintenance et des performances	201

8.3	Modification et réadaptation	201
8.4	Retrait du service et dépose	201
Annexe A (normative)	Niveaux d'intégrité de sécurité	202
A.1	Généralités	202
A.2	Exigences de sécurité	202
A.3	Intégrité de la sécurité	203
A.4	Détermination des exigences d'intégrité de la sécurité	204
A.4.1	Généralités	204
A.4.2	Appréciation du risque	205
A.4.3	Maîtrise des dangers	207
A.4.4	Identification et traitement des nouveaux dangers apparaissant au cours de la conception	213
A.5	Allocation de SIL	214
A.5.1	Aspects généraux	214
A.5.2	Relation entre un SIL et le TFFR associé	215
Annexe B (normative)	Gestion des pannes des fonctions relatives à la sécurité	217
B.1	Généralités	217
B.2	Concepts généraux	217
B.2.1	Temps de détection et de passivation	217
B.2.2	Composition de deux entités indépendantes	218
B.3	Effets des pannes	219
B.3.1	Effets des pannes simples	219
B.3.2	Indépendance des entités	221
B.3.3	Détection de pannes simples	226
B.3.4	Action suivant la détection (maintien dans un état sûr)	229
B.3.5	Effets des pannes multiples	231
B.3.6	Protections contre les pannes systématiques	234
Annexe C (normative)	Identification des modes de défaillance des composants matériels	235
C.1	Généralités	235
C.2	Procédure générale	235
C.3	Procédure pour les circuits intégrés	235
C.4	Procédure pour les composants avec propriétés physiques intrinsèques	236
C.5	Dispositions générales concernant les modes de défaillance des composants	236
Annexe D (informative)	Exemple d'allocation des THR/TFFR/FR et des SIL	254
Annexe E (normative)	Techniques et mesures pour éviter les pannes systématiques et maîtriser les pannes systématiques et aléatoires	256
E.1	Généralités	256
E.2	Tableaux des techniques et mesures	258
Annexe F (informative)	Recommandations relatives aux circuits intégrés programmables par l'utilisateur	266
F.1	Généralités	266
F.1.1	Objet	266
F.1.2	Terminologie et contexte	266
F.2	Cycle de vie de l'UPIC	267
F.2.1	Généralités	267
F.2.2	Organisation, rôles, responsabilités et compétences du personnel	270
F.2.3	Exigences de l'UPIC	270

F.2.4	Architecture et conception de l'UPIC.....	270
F.2.5	Conception des composants logiques	271
F.2.6	Codage des composants logiques.....	271
F.2.7	Vérification des composants logiques	271
F.2.8	Réalisation physique de l'UPIC	271
F.2.9	Intégration de l'UPIC	272
F.2.10	Validation de l'UPIC.....	272
F.2.11	Exigences pour l'utilisation de composants logiques préexistants	272
F.3	Exigences techniques détaillées applicables à un UPIC	272
F.3.1	Recommandations relatives à l'architecture de la sécurité	272
F.3.2	Protection contre les pannes aléatoires — principes architecturaux	272
F.3.3	Protection contre les pannes systématiques – techniques et mesures	273
Annexe G (informative) Modifications apportées au présent document par rapport à l'IEC 62425:2007		282
Bibliographie.....		285
Figure 1	— Domaine d'application des normes ferroviaires de l'IEC et du CENELEC	151
Figure 2	— Structure de l'IEC 62425.....	165
Figure 3	— Exemple de cycle de vie du système	167
Figure 4	— Exemple de la partie conception et validation du cycle de vie du système	169
Figure 5	— Indépendance des rôles pour différents SIL et niveaux d'intégrité de base (BI) – phases 5 à 10	171
Figure 6	— Plan du dossier de sécurité.....	185
Figure 7	— Plan du rapport de sécurité technique.....	187
Figure 8	— Exemples d'utilisation possible des dossiers de sécurité.....	197
Figure 9	— Exemples de différents processus d'acceptation de la sécurité	200
Figure A.1	— Exigences de sécurité et intégrité de la sécurité	203
Figure A.2	— Le modèle du sablier	205
Figure A.3	— Définition des dangers à l'égard des limites du système	207
Figure A.4	— Exemple de processus analyse des situations dangereuses	209
Figure A.5	— Défaillances de cause commune (CCF)	211
Figure A.6	— Traitement générique des défaillances de cause commune selon l'analyse par arbre de panne.....	212
Figure A.7	— Liens entre les SIL et les techniques	215
Figure B.1	— Temps de détection et de passivation.....	217
Figure B.2	— Maîtrise des pannes simples et multiples.....	221
Figure B.3	— Influences affectant l'indépendance d'entités.....	223
Figure B.4	— Détection et passivation de pannes simples – Sécurité composite	230
Figure B.5	— Détection et passivation de pannes simples – Sécurité réactive	230
Figure C.1	— Exemple de résistance à 4 sorties utilisant une technique hybride couche épaisse.....	238
Figure D.1	— Exemple d'allocation des THR/TFFR/FR et des SIL associés	254
Figure F.1	— Architecture de l'UPIC	267
Figure F.2	— Contexte de développement de l'UPIC.....	267
Figure F.3	— Exemple de cycle de vie du développement d'un UPIC	268
Figure F.4	— Exemple de cycle de vie du développement d'un UPIC avec des composants préexistants	269
Figure F.5	— Techniques et mesures de développement d'un UPIC	274

Tableau 1 — Exemple de modèle de SRAC	178
Tableau 2 – Sections et contenu du rapport de sécurité technique	187
Tableau A.1 — Table des SIL	216
Tableau B.1 — Mesures de détection des pannes dans les circuits intégrés par des essais périodiques en ligne	232
Tableau C.1 — Résistances	238
Tableau C.2 — Condensateurs	239
Tableau C.3 — Composants électromagnétiques	240
Tableau C.4 — Diodes	243
Tableau C.5 — Transistors	244
Tableau C.6 — Redresseurs contrôlés	246
Tableau C.7 — Suppresseurs de surtension	247
Tableau C.8 — Composants optoélectroniques	248
Tableau C.9 — Filtres	250
Tableau C.10 — Assemblages d'interconnexion	251
Tableau C.11 — Fusibles	252
Tableau C.12 — Interrupteurs et boutons poussoirs	252
Tableau C.13 — Lampes	252
Tableau C.14 — Batteries	253
Tableau C.15 – Transducteurs et capteurs (à l'exclusion de ceux comportant un circuit électronique intégré)	253
Tableau E.1 — Activités de planification et d'assurance qualité de la sécurité	258
Tableau E.2 — Spécification des exigences de sécurité	259
Tableau E.3 — Organisation de la sécurité	259
Tableau E.4 — Architecture du système, sous-système ou équipement	260
Tableau E.5 — Caractéristiques de conception	261
Tableau E.6 — Méthodes d'analyse des situations dangereuses et des défaillances	262
Tableau E.7 — Conception et développement du système, sous-système ou équipement	263
Tableau E.8 — Vérification et validation de la sécurité du système, sous-système ou équipement	264
Tableau E.9 — Application, exploitation et maintenance	265
Tableau F.1 — Exemple de documentation produite à chaque phase	269
Tableau F.2 — Techniques et mesures simplifiées pour la protection contre les défaillances systématiques	274
Tableau F.3 — Conception et vérification (y compris toutes les activités préalables à la synthèse)	275
Tableau F.4 — Synthèse	275
Tableau F.5 — Placement, routage et agencement	276
Tableau F.6 — Description des techniques de conception	276
Tableau F.7 — Description des techniques de synthèse	280
Tableau F.8 — Description des techniques de placement, de routage et d'agencement	281
Tableau G.1 — Articles et paragraphes — Correspondance avec l'IEC 62425:2007	282
Tableau G.2 — Figures et tableaux — Correspondance avec l'IEC 62425:2007	284

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATION ET DE TRAITEMENT – SYSTÈMES ÉLECTRONIQUES DE SÉCURITÉ POUR LA SIGNALISATION

AVANT-PROPOS

- 1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications ; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'IEC attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, l'IEC n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse <https://patents.iec.ch>. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 62425 a été établi par le comité d'études 9 de l'IEC : Matériels et systèmes électriques ferroviaires. Il s'agit d'une Norme internationale.

L'EN 50129:2018 a servi de base à l'élaboration du présent document.

Cette deuxième édition annule et remplace la première édition parue en 2007. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- a) le document a été aligné sur les phases du cycle de vie définies dans l'IEC 62278-1 ;
- b) l'Article 5 décrit les exigences relatives au développement de systèmes électroniques relatifs à la sécurité (jusqu'à la phase 9 du cycle de vie) ;
- c) l'Article 8 traite des exigences relatives à l'acceptation et à l'approbation de la sécurité des systèmes électroniques relatifs à la sécurité, ainsi que des phases suivantes du cycle de vie ;
- d) des exigences et des recommandations ont été ajoutées à l'Article 6 concernant les sujets suivants :
 - 1) réutilisation de systèmes préexistants ;
 - 2) outils relatifs à la sécurité ;
 - 3) impact des menaces de cybersécurité sur la sécurité fonctionnelle ;
 - 4) dossiers de sécurité pour applications spécifiques ;
- e) les exigences relatives à la structure et au contenu du dossier de sécurité sont désormais définies dans un Article 7 dédié ;
- f) l'Annexe A a été mise à jour en ce qui concerne la spécification et l'allocation des exigences d'intégrité de la sécurité ;
- g) le contenu de l'ancienne Annexe D a été fusionné avec celui de l'Annexe B, et l'annexe est passée du statut informatif à normatif ;
- h) l'Annexe E est passée du statut informatif à normatif ;
- i) une Annexe F informative a été ajoutée pour couvrir les circuits intégrés programmables par l'utilisateur.

L'Annexe G compare en détail les modifications entre l'IEC 62425:2007 et le présent document.

La présente version bilingue (2025-11) correspond à la version anglaise monolingue publiée en 2025-10.

La version française de cette norme n'a pas été soumise au vote.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détails à l'adresse www.iec.ch/standardsdev/publications.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé, ou
- révisé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de ce document indique qu'il contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

La présente Norme internationale définit les exigences pour le développement et l'acceptation des systèmes électroniques relatifs à la sécurité dans le domaine de la signalisation ferroviaire.

Les systèmes électroniques relatifs à la sécurité pour la signalisation incluent les aspects matériel et logiciel. Pour développer des systèmes relatifs à la sécurité complets, ces deux aspects doivent être pris en compte tout au long du cycle de vie du système. Les exigences concernant le système électronique global relatif à la sécurité et ses aspects matériels sont définies dans le présent document. Les autres exigences sont définies dans les normes de l'IEC et du CENELEC associées. Pour les systèmes relatifs à la sécurité comprenant des logiciels, des conditions supplémentaires sont définies dans l'IEC 62279:2015.

NOTE 1 L'IEC 62279:2015 est basée sur la Norme européenne EN 50128:2011.

Des exigences supplémentaires pour la communication relative à la sécurité sont définies dans l'IEC 62280:2014.

Le présent document est le référentiel commun pour l'acceptation et l'approbation de la sécurité des systèmes électroniques utilisés dans les applications de signalisation ferroviaire. Le but des sociétés d'exploitation ferroviaire et de l'industrie ferroviaire est de développer des systèmes ferroviaires basés sur des normes communes. Les autorités de tutelle compétentes peuvent appliquer le présent document aux domaines pertinents qu'elles choisissent. Sur cette base, l'acceptation réciproque des approbations de la sécurité pour des sous-systèmes et équipements peut être appliquée par les différentes autorités de tutelle nationales.

L'acceptation réciproque s'applique à l'approbation générique et non à des applications spécifiques.

Le présent document concerne les preuves à fournir pour l'acceptation des systèmes relatifs à la sécurité. Toutefois, il spécifie non seulement les activités du cycle de vie qui doivent être terminées avant la phase d'acceptation, mais également les activités planifiées supplémentaires à réaliser après. De cette manière, la justification de la sécurité couvre l'ensemble du cycle de vie.

Le présent document précise quelles sont les preuves qui doivent être établies. Sauf si cela est considéré comme opportun, il ne spécifie pas qui réalise le travail requis. Le travail requis peut être effectué par différentes personnes, dans différentes circonstances ou structures organisationnelles, sous réserve que l'indépendance des rôles soit respectée.

Le présent document se compose des Articles 1 à 8, qui constituent le corps principal du document, ainsi que des Annexes A, B, C, D, E, F et G. Les exigences définies des Articles 5 à 8 du présent document et dans les Annexes A, B, C et E sont normatives, tandis que les Annexes D, F et G sont informatives.

Le présent document est aligné sur l'IEC 62278-1:—¹ et l'IEC 62278-2:—¹, et contient des références à ces normes.

NOTE 2 L'IEC 62278-1:— et l'IEC 62278-2:— sont basées sur les Normes européennes EN 50126-1:2017 et EN 50126-2:2017 respectivement.

¹

En cours d'élaboration. Stade au moment de la publication : IEC/FDIS 62278-1:2025 et IEC/FDIS 62278-2:2025.

Le présent document est basé sur le cycle de vie du système décrit dans la série IEC 62278 et est aligné sur la série IEC 61508. L'IEC 62278, l'IEC 62279 et l'IEC 62425 couvrent le secteur ferroviaire de manière équivalente à la série EN 61508 en ce qui concerne les systèmes ferroviaires de signalisation, de télécommunication et de traitement. Étant donné que la conformité à ces documents a été démontrée, le présent document ne contient aucune exigence prévoyant d'évaluer à nouveau la conformité à la série IEC 61508.

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATION ET DE TRAITEMENT – SYSTÈMES ÉLECTRONIQUES DE SÉCURITÉ POUR LA SIGNALISATION

1 Domaine d'application

Le présent document s'applique aux systèmes électroniques relatifs à la sécurité (en incluant les sous-systèmes et les équipements) utilisés dans les applications de signalisation ferroviaire.

Le présent document s'applique aux systèmes génériques (c'est-à-dire aux produits ou systèmes génériques qui définissent une classe d'applications), ainsi qu'aux systèmes destinés à des applications spécifiques.

La Figure 1 représente le domaine d'application du présent document, ainsi que ses relations avec les autres normes de l'IEC et du CENELEC.

Le présent document est applicable uniquement à la sécurité fonctionnelle des systèmes. Il ne traite pas d'autres aspects de la sécurité tels que la santé des travailleurs et la sécurité du personnel. Si la sécurité fonctionnelle des systèmes peut avoir un impact sur la sécurité du personnel, la santé et la sécurité des travailleurs peuvent également être affectées par d'autres aspects de la conception du système qui ne sont pas couverts par le présent document. Les aspects de cybersécurité de la sécurité fonctionnelle ne sont couverts que dans une certaine mesure.

Le présent document s'applique à toutes les phases du cycle de vie d'un système électronique relatif à la sécurité, et en particulier aux phases 5 (architecture et allocation des exigences du système) à 10 (acceptation du système) définies dans l'IEC 62278-1:—.

Les exigences applicables aux systèmes non relatifs à la sécurité ne relèvent pas du domaine d'application du présent document.

Le présent document n'est pas applicable aux systèmes, sous-systèmes ou équipements existants (c'est-à-dire ceux qui ont déjà été acceptés avant le développement du présent document). Toutefois, autant que cela est raisonnablement possible, le présent document s'applique aux modifications et extensions des systèmes, sous-systèmes et équipements existants.

Le présent document s'applique essentiellement aux systèmes, sous-systèmes ou équipements qui ont été spécialement conçus et fabriqués dans les applications de signalisation ferroviaire. Le présent document s'applique également, autant que cela est raisonnablement possible, aux équipements généraux ou industriels (par exemple, alimentations, écrans d'affichage ou autres articles disponibles dans le commerce) qui sont utilisés comme partie d'un système électronique relatif à la sécurité.

Le présent document s'adresse aux responsables d'exploitation ferroviaire, aux fournisseurs de matériel ferroviaire et aux chargés d'évaluations ainsi qu'aux autorités de tutelle, même si ce document ne définit pas un processus d'approbation applicable par les autorités de tutelle.

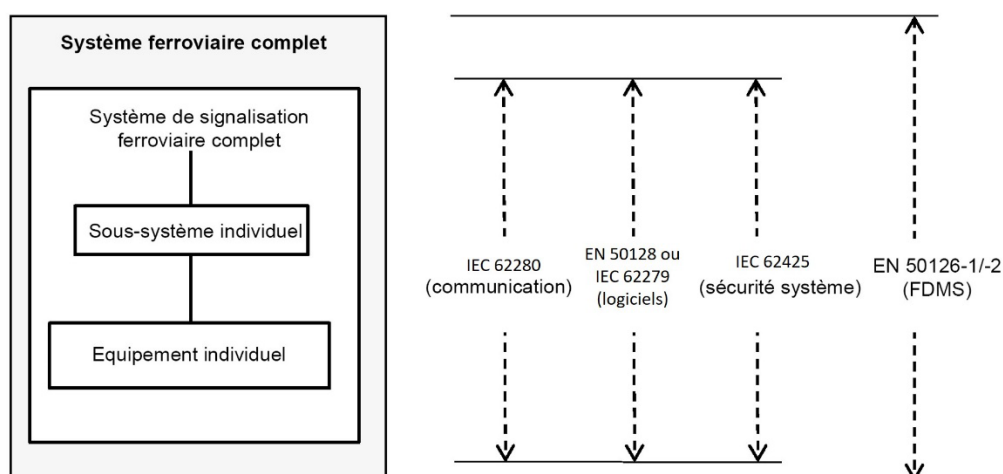


Figure 1 — Domaine d'application des normes ferroviaires de l'IEC et du CENELEC

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60664-1:2020, *Coordination de l'isolement des matériels dans les réseaux d'énergie électrique à basse tension — Partie 1 : Principes, exigences et essais*

IEC 62278-1:—², *Applications ferroviaires — Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) — Partie 1 : Processus FMDS générique*

IEC 62278-2:—², *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*

IEC 62279:2015, *Applications ferroviaires — Systèmes de signalisation, de télécommunication et de traitement — Logiciels pour systèmes de commande et de protection ferroviaire*

IEC 62280:2014, *Applications ferroviaires — Systèmes de signalisation, de télécommunication et de traitement — Communication de sécurité dans les systèmes de transmission*

IEC 62497-1³:2010, *Applications ferroviaires — Coordination de l'isolement — Partie 1 : Exigences fondamentales — Distances d'isolement dans l'air et lignes de fuite pour tout matériel électrique et électronique*
IEC 62497-1:2010/AMD1:2013

² En cours d'élaboration. Stade au moment de la publication : IEC/FDIS 62278-1:2025 et IEC/FDIS 62278-2:2025.

³ Il existe une édition 1.1:2013 consolidée, qui inclut l'IEC 62497-1:2010 ainsi que son Amendement 1:2013.

IEC 62498-1:2010, *Applications ferroviaires — Conditions d'environnement pour le matériel — Partie 1 : Équipement embarqué du matériel roulant*

IEC 62498-3:2010, *Applications ferroviaires — Conditions d'environnement pour le matériel — Partie 3 : Équipement pour la signalisation et les télécommunications*