IEC 62425

Edition 2.0 2025-05

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

ICS 45.060.01

ISBN 978-2-8327-0796-8

IEC 62425:2025-05(en-fr)



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 Varembé
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 It also gives information on projects, replaced and withdrawn publications.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.

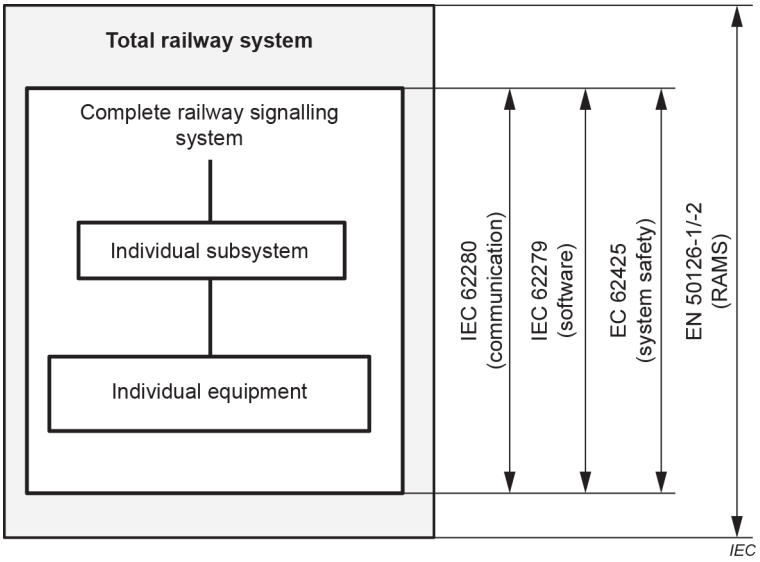


Figure 1 – Scope of the main IEC and CENELEC railway application standards

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 62497-1[3]: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.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

3.1.1
accident
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”]

3.1.2
basic insulation
insulation of hazardous-live-parts which provides basic protection

Note 1 to entry: This concept does not apply to insulation used exclusively for functional purposes.

[SOURCE: IEC 60050-826:2021, 826-12-14, modified – The words “of hazardous live-parts” have been added.]

3.1.3
basic integrity
integrity attribute for a safety-related function with a tolerable functional failure rate equal to, or higher than (less demanding), 10^{-5} h^{-1}; or for a non-safety-related function

Note 1 to entry: In this document basic integrity requirements relate only to safety-related functions. If a non-safety-related function has been given basic integrity requirements on the basis of the process described in IEC 62278-1:—, no additional requirements are defined in this document.

[SOURCE: IEC 62278-1:—, 3.7, modified – "Note 1 to entry has been added.]

3.1.4
causal analysis
analysis of the reasons how and why a particular hazard can come into existence

[SOURCE: IEC 60050-821:2017, 821-12-07]

3.1.5
common cause failures, pl
failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause

[SOURCE: IEC 60050-192:2015, 192-03-18, modified – Notes 1 and 2 to entry have been deleted.]

3.1.6
configuration
structuring and interconnection of the hardware and software of a system for its intended application

[SOURCE: IEC 60050-821:2017, 821-12-12]

3.1.7
consequence analysis
analysis of events which are likely to happen after a hazard has occurred

[SOURCE: IEC 60050-821:2017, 821-12-14]

3.1.8
cross-acceptance
status achieved by a product that has been accepted by one authority to the relevant standards and is acceptable to other authorities without the necessity for further assessment

[SOURCE: IEC 60050-821:2017, 821-12-15]

3.1.9
DC fault model
fault category that includes the following failure modes: stuck-at faults, stuck-open, open or high impedance outputs and short circuit between signal lines, and for integrated circuits short circuit between any two connections (pins)

3.1.10
design
activity applied in order to analyse and transform specified requirements into acceptable solutions

[SOURCE: IEC 60050-821:2017, 821-12-16, modified – The end of the definition "design solutions which have the required safety integrity level" has been replaced with "solutions".]

3.1.11
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 failures. 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, modified – The supplementary information has been moved to a new note 1 to entry, which replaces the original note 1 to entry.]

3.1.12
double insulation
insulation comprising both basic insulation and supplementary insulation

Note 1 to entry: In double insulation, each layer shall be able to be tested or analysed separately. In particular:

– the clearance distance shall be the basic distance. In addition, also the supplementary solid layer shall be dimensioned taking into account the same rated impulse voltage (U_{Ni}).

– the creepage distance shall be the sum of basic and supplementary distances. The basic distance shall be evaluated against the rated insulation voltage (U_{Nm}). In addition, also the supplementary distance shall be evaluated against the same U_{Nm}. The U_{Nm} shall not be apportioned.

Note 2 to entry: With respect to Note 1, for definition of rated insulation voltage and rated impulse voltage, see IEC 62497-1:2010 and IEC 62497-1:2010/AMD1:2013. Similar definitions can also be found in IEC 60664-1:2020.

[SOURCE: IEC 60050-195:2021, 195-06-08, modified – Notes to entry 1 and 2 have been added.]

3.1.13
electronic component
hardware component
electronic device that cannot be taken apart without destruction or impairment of its intended use

EXAMPLE: Resistors, capacitors, diodes, integrated circuits, hybrids, application specific integrated circuits, wound components and relays.

[SOURCE: IEC 60050-904:2014, 904-01-09, modified – The preferred terms "electronic part" and "piece part" have been deleted and a new preferred term "hardware component" has been added.]

3.1.14
equipment
single apparatus or set of devices or apparatuses, or the set of main devices of an installation, or all devices necessary to perform a specific task

Note 1 to entry: Examples of equipment are a power transformer, the equipment of a substation, measuring equipment.

[SOURCE: IEC 60050-151:2001, 151-11-25]

3.1.15
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, modified – Notes 1 and 2 to entry have been modified.]

3.1.16
fail-safe
able to enter or remain in a safe state in the event of a failure

[SOURCE: IEC 60050-821:2017, 821-01-10]

3.1.17
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.

[SOURCE: IEC 60050-821:2017, 821-11-19, modified – Note 3 to entry has been added.]

3.1.18
failure rate
limit of the ratio of the conditional probability that the instant of time, T, of a failure of a product falls within a given time interval (t, t + Δt) and the duration of this interval, Δt, when Δt tends towards zero, given that the item is in an up state at the start of the time interval

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

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

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

3.1.19
fault
<in a system> abnormal condition that can lead to an error in a system

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

[SOURCE: IEC 60050-821:2017, 821-11-20]

3.1.20
fault detection time
time interval between failure and detection of the resulting fault

[SOURCE: IEC 60050-192:2015, 192-07-11, modified – The deprecated term “undetected fault time” as well as Figures 1 and 2 have been deleted.]

3.1.21
function
<of an item> specified action or activity which can be performed by technical means 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.

3.1.22
functional safety
part of the overall safety that depends on functional and physical units operating correctly in response to their inputs

[SOURCE: IEC 60050-351:2013, 351-57-06, modified – Note 1 to entry has been deleted.]

3.1.23
harm
injury or damage to the health of people, or damage to property or the environment.

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

3.1.24
hazard
<in railway> condition that can 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".

3.1.25
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

[SOURCE: IEC 60050-821:2017, 821-11-23]

3.1.26
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]

3.1.27
implementation
activity applied in order to transform the specified designs into their realization

[SOURCE: IEC 60050-821:2017, 821-12-29, modified – “physical realization" changed to "realization".]

3.1.28
independence of roles
freedom from involvement in the same intellectual, commercial or management entity

3.1.29
independent safety assessment
process to determine whether the system or product meets the specified safety requirements and to form a judgement as to whether the system or product is fit for its intended purpose in relation to safety

[SOURCE: IEC 62278-1:—, 3.33, modified – Note 1 to entry has been deleted.]

3.1.30
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]

3.1.31
negation
enforcement of a safe state following detection of a hazardous fault

[SOURCE: IEC 60050-821:2017, 821-12-38]

3.1.32
negation time
time interval which begins when the existence of a fault is detected and ends when a safe state is enforced

[SOURCE: IEC 60050-821:2017, 821-12-39]

3.1.33
pre-existing item
item that already exists and that was not developed specifically for the current project

3.1.34
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, modified – The specific use "in signalling" has been made more general with "in railway".]

3.1.35
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 or maintainers 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.

[SOURCE: IEC 62278-1:—, 3.48]

3.1.36
random failure integrity
degree to which a system is free from hazardous random faults

Note 1 to entry: This definition can be read as "integrity from failures due to random faults".

[SOURCE: IEC 60050-821:2017, 821-12-45, modified – Note 1 to entry has been added.]

3.1.37
random fault
unpredictable occurrence of a fault

[SOURCE: IEC 60050-821:2017, 821-12-46]

3.1.38
redundancy
<in a system> provision of more than one means for performing a function

[SOURCE: IEC 60050-192:2015, 192-10-02, modified – Note 1 to entry has been deleted.]

3.1.39
reinforced insulation
insulation of hazardous-live-parts which provides a degree of protection against electric shock equivalent to double insulation

Note 1 to entry: Reinforced insulation may comprise several layers which cannot be tested singly as basic insulation or supplementary insulation.

[SOURCE: IEC 60050-581:2008, 581-21-27]

3.1.40
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., and the units should always be clearly stated.

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 IEC 60050-192:2015, Section 192-05: Reliability related concepts: measures.

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

3.1.41
repair
direct action taken to effect restoration

Note 1 to entry: Repair includes fault localization (IEV 192-06-19), fault diagnosis (IEV 192-06-20), fault correction (IEV 192-06-21), and function checkout (IEV 192-06-22).

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

3.1.42
risk
<for railway safety> combination of the frequency of occurrence of harm and the severity of that harm

3.1.43
safe state
condition which continues to preserve safety

[SOURCE: IEC 60050-821:2017, 821-12-49]

3.1.44
safety
freedom from unacceptable risk

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

3.1.45
safety acceptance
safety status given to a product by the final user

[SOURCE: IEC 60050-821:2017, 821-12-50]

3.1.46
safety approval
safety status given to a product by the requisite authority when the product has fulfilled a set of pre-determined conditions

[SOURCE: IEC 60050-821:2017, 821-12-51]

3.1.47
safety authority
body responsible for delivering the authorization for the operation of the safety-related system

[SOURCE: IEC 60050-821:2017, 821-12-52]

3.1.48
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]

3.1.49
safety function
function whose sole purpose is to ensure safety

Note 1 to entry: All safety functions are safety-related functions, but not vice versa.

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

[SOURCE: IEC 62278-1:—, 3.67]

3.1.50
safety integrity
ability of a safety-related system or product to achieve its required safety-related functions under all the stated conditions within a stated operational environment and within a stated duration

[SOURCE: IEC 60050-821:2017, 821-12-54, modified – “or product” has been added; “safety functions” has been changed to “safety-related functions”.]

3.1.51
safety integrity level
one of a number of defined discrete levels for specifying the safety integrity requirements of 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.

[SOURCE: IEC 62278-1:—, 3.69]

3.1.52
safety life cycle
additional series of activities carried out in conjunction with the system life cycle for safety-related systems

[SOURCE: IEC 60050-821:2017, 821-12-55]

3.1.53
safety plan
documented set of time scheduled activities, resources and events serving to implement the organization, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given safety requirements relevant to a given contract or project

[SOURCE: IEC 60050-821:2017, 821-12-57]

3.1.54
safety process
series of procedures that are followed to enable all safety requirements of a product to be identified and met

[SOURCE: IEC 60050-821:2017, 821-12-58]

3.1.55
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.

[SOURCE: IEC 60050-821:2017, 821-01-73, modified – Note 1 to entry has been added.]

3.1.56
signalling system
system to ensure the safe movement of trains

Note 1 to entry: For the purposes of this document, railway signalling applications encompass all systems which control and protect train movements by conveying instructions or warnings to trains or trackside systems. Where a signalling system includes subsystems or equipment on board of the train, this document is intended to apply up to the interface with the braking system, traction control system or other relevant train systems.

[SOURCE: IEC 60050-821:2017, 821-01-03, modified – The end of the definition "by means of one or more of the following: lineside indications, wayside/onboard data exchange, indications given in the driver's cab" has been omitted and Note 1 to entry has been added.]

3.1.57
stress profile
degree and number of external influences which a system can withstand whilst performing its required functionality

[SOURCE: IEC 60050-821:2017, 821-12-65]

3.1.58
subsystem
part of a system, which is itself a system

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

3.1.59
supplementary insulation
independent insulation applied in addition to basic insulation, that provides fault protection

[SOURCE: IEC 60050-195:2021, 195-06-07]

3.1.60
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, modified – Notes to entry have been deleted.]

3.1.61
system life cycle
activities occurring during a given time interval that starts when a system is conceived and ends when the system is no longer available for use, is decommissioned and is disposed of

[SOURCE: IEC 60050-821:2017, 821-12-66]

3.1.62
systematic failure integrity
degree to which a system is free from hazardous systematic faults

Note 1 to entry: This definition can be read as "integrity from failures due to systematic faults", in analogy with IEC 60050-821:2017, 821-12-46, where "random" is replaced by "systematic".

[SOURCE: IEC 60050-821:2017, 821-12-68, modified – In the the definition, "unidentified hazardous errors and the causes thereof" has been replaced with "hazardous systematic faults" and note 1 to entry has been added.]

3.1.63
systematic fault
<in signalling> inherent fault in the specification, design, construction, installation, operation or maintenance of a system, subsystem or equipment

[SOURCE: IEC 60050-821:2017, 821-12-69]

3.1.64
technical safety report
documented technical evidence for the safety of the design of a system, subsystem or equipment

Note 1 to entry: The technical safety report is part of the safety case.

[SOURCE: IEC 60050-821:2017, 821-12-70, modified – Note 1 to entry has been added.]

3.1.65
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: Multiple validations can be carried out if there are different intended uses.

[SOURCE: IEC 60050-192:2015, 192-01-18, modified – Original Note 4 to entry has been deleted and Note 5 became Note 4.]

3.1.66
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, modified – Note 3 to entry has been modified: "In the case of software," has been deleted; "software and its constituents" has been replaced by "system and its constituents"; “stage” has been changed to “life cycle phase”.]

3.2 Abbreviated terms

CCF	common cause failures
COTS	commercial off the shelf
DES	designer
DT	down time, T_D + T_N + T_R
EMC	electromagnetic compatibility
EMI	electromagnetic interference
ESD	electrostatic discharge
FFR	functional failure rate
FMEA	failure modes and effects analysis
FR	failure rate
FTA	fault tree analysis
GA	generic application
GP	generic product
HAZOP	hazard and operability study
HDL	hardware description language
HW	hardware
GASC	generic application safety case
GPSC	generic product safety case
IP	intellectual property