This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

2026-05-18

Jernbaner – Telekommunikationsteknik, signalteknik og databehandlingssystemer – Sikkerhedsrelaterede elektroniske systemer for signalteknik

Railway Application – Communication, signalling and processing system – Safety related electronic systems for signalling

DANSK STANDARD
Danish Standards Association

Göteborg Plads 1
DK-2150 Nordhavn

Tel: +45 39 96 61 01
dansk.standard@ds.dk
www.ds.dk

© Dansk Standard - Eftertryk uden tilladelse forbudt

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

DS/EN 50129:2026

København
DS projekt: M387932
ICS: 93.100

Første del af denne publikations betegnelse er:
DS/EN, hvilket betyder, at det er en europæisk standard, der har status som dansk standard.

Denne publikations overensstemmelse er:
IDT med: EN 50129:2026

Denne publikation erstatter: DS/EN 50129:2018, DS/EN 50129:2018/AC:2019

I tilfælde af redaktionelle fejl i DS-publikationen kan der skrives til:
editorial-mistakes@ds.dk

ADVARSEL: DS-publikationer revideres over tid. Derudover kan sådanne publikationer ændres ved rettelsesblade og/eller tillæg. Der kan også udgives rettelsesblade, der udelukkende angår oversættelsen af en publikation. Det er derfor vigtigt at sikre sig, at man benytter en gældende udgave, medmindre fx lovgivning kræver andet. Den enkelte publikations status fremgår af https://webshop.ds.dk/. Her kan man desuden tilmelde sig en gratis notifikationsservice og følge en udgivet DS-publikations udvikling ved at klikke på "Følg".

En oversigt over forskellige DS-publikationstyper og -betegnelser findes her:
https://www.ds.dk/publikationstyper

Indholdet i dette dokument er ophavsretligt beskyttet, herunder tekst, grafik, billeder og lyd. Fonden Dansk Standard forbeholder sig udtrykkeligt alle rettigheder til at udnytte indholdet til tekst- og datamining, jf. ophavsretslovens § 11 b, stk. 2, og artikel 4 i direktiv (EU) 2019/790. Enhver udnyttelse af indholdet i dette dokument til tekst- og dataminingformål kræver forudgående skriftlig, specifik tilladelse fra Fonden Dansk Standard.

In case of editorial errors in the DS publication, please write to:
editorial-mistakes@ds.dk

NOTICE: DS publications are revised over time. In addition, such publications may be altered by corrigenda and/or amendments. Also, corrigenda may be published solely in relation to the translation of a publication. It is therefore important to ensure that the edition used is valid, unless, for example, legislation requires otherwise. The status of each publication can be found at https://webshop.ds.dk/. Here you can also sign up for a free notification service and follow the progress of a published DS publication by clicking on "Follow".

An overview of different DS publication types and designations can be found here:
https://www.ds.dk/publikationstyper

The content of this document, including text, graphics, images, and audio, is protected by copyright. The Danish Standards Foundation explicitly reserves all rights regarding the use of its content for text and data mining purposes in accordance with Section 11b(2) of the Danish Copyright Act and Article 4 of Directive (EU) 2019/790. Any use of the content of this document for text and data mining purposes requires prior, written, specific permission from the Danish Standards Foundation.

EUROPEAN STANDARD **EN 50129**

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

EUROPÄISCHE NORM

May 2026

ICS 93.100

Supersedes EN 50129:2018; EN 50129:2018/AC:2019-04

English Version

Railway Application - Communication, signalling and processing system - Safety related electronic systems for signalling

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

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsbezogene elektronische Systeme für Signaltechnik

This European Standard was approved by CENELEC on 2026-04-20. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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



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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2026 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN 50129:2026 E

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

Contents

Page

European foreword 4
Introduction 5
1 Scope 6
2 Normative references 7
3 Terms, definitions and abbreviated terms 7
3.1 Terms and definitions 7
3.2 Abbreviated terms 18
4 Overall framework of this document 19
5 Requirements for developing safety-related electronic systems 21
5.1 General 21
5.2 The quality management process 21
5.3 The safety management process 23
6 Requirements for elements following different life cycles 35
6.1 General 35
6.2 Use of pre-existing items 35
6.3 Safety-related tools for electronic systems 37
6.4 Physical security and cybersecurity 39
7 The safety case: structure and content 41
7.1 The safety case structure 41
7.2 The technical safety report 42
7.3 Generic and specific safety cases 50
7.4 Provisions for the specific application safety case 51
7.5 Dependencies between safety cases 52
7.6 Safety report for Basic Integrity functions 52
8 System safety acceptance and subsequent phases 53
8.1 System safety acceptance process 53
8.2 Operation, maintenance and performance monitoring 57
8.3 Modification and retrofit 57
8.4 Decommissioning and disposal 57
Annex A (normative) Safety Integrity Levels 58
A.1 General 58
A.2 Safety requirements 58
A.3 Safety Integrity 59
A.4 Determination of Safety Integrity requirements 60
A.5 Allocation of SILs 70
Annex B (normative) Management of faults for safety-related functions 73
B.1 General 73
B.2 General concepts 73
B.3 Effects of faults 75
Annex C (normative) Identification of hardware component failure modes 89
C.1 General 89

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

C.2 General procedure 89
C.3 Procedure for integrated circuits 89
C.4 Procedure for components with inherent physical properties 90
C.5 General provisions concerning component failure modes 90
Annex D (informative) Example of THR/TFFR/FR apportionment and SIL allocation 108
Annex E (normative) Techniques and measures for the avoidance of systematic faults and the control of random and systematic faults 110
E.1 General 110
E.2 Tables of techniques and measures 112
Annex F (informative) Guidance on User Programmable Integrated Circuits 120
F.1 General 120
F.2 UPIC life cycle 121
F.3 Detailed technical requirements for UPIC 126
Annex G (informative) Changes in this document compared to EN 50129:2018 136
Bibliography 139

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

European foreword

This document (EN 50129:2026) has been prepared by CLC/SC 9XA “Communication, signalling and processing systems” of CLC/TC 9X “Electrical and electronic applications for railways”.

The following dates are fixed:

- latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2027-05-31
- latest date by which the national standards conflicting with this document have to be withdrawn (dow) 2029-05-31

This document supersedes EN 50129:2018 and all of its amendments and corrigenda (if any).

EN 50129:2026 includes the following significant technical changes with respect to EN 50129:2018.

Requirements and guidance have been added on the following topics:

— Clause 5: update of requirements and guidance on safety qualification tests;

— Clause 6: update of requirements and guidance on safety-related tools, cybersecurity;

— Clause 7: update of requirements and guidance on cybersecurity; a significant portion of 7.2 has been incorporated into Table 2;

— Annex C: update of insulation coordination requirements for better readability;

— Annex E: a new column has been added for Basic Integrity.

A more detailed comparison of changes between EN 50129:2018 and this document can be found in Annex G.

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

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

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

Introduction

This document 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 CENELEC standards.

General requirements for a consistent approach to the management of RAMS are given in EN 50126-1:2017 and EN 50126-2:2017. For safety-related systems which include software, additional requirements are defined in EN 50716:2023. Additional requirements for safety-related communication are defined in EN 50159:2010.

Cyberattacks can affect the safety of a system, but this document does not specify the cybersecurity requirements for the development, implementation, maintenance and operation of security policies, services, or systems. For cybersecurity, appropriate standards apply.

NOTE ISO/IEC and CEN/CENELEC publications that address cybersecurity in depth are EN ISO/IEC 27000 and ISO/IEC TR 19791. In the field of industrial automation and control systems, the EN IEC 62443 series have been defined. CLC/TS 50701:2023 addresses cybersecurity for the railway domain and was derived from the EN IEC 62443 series.

The aim of European railway duty holders and of European railway industry is to develop compatible railway systems based on common standards. Therefore cross-acceptance of safety approvals for systems, subsystems or equipment by the different national railway duty holders is needed. This document is the common European base for safety acceptance of electronic systems for railway signalling applications.

Cross-acceptance is aimed at the acceptance of generic products or generic applications that can be used for a number of different specific applications, and not at the acceptance of any single specific application. Public procurement within the European Community concerning safety-related electronic systems for railway signalling applications will refer to this document.

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 system acceptance phase, 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 Clause 1 to Clause 8, which form the main part, and Annexes A, B, C, D, E, F and G . The requirements defined in Clause 5 to Clause 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 contains references to:

— EN 50126-1:2017, Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Generic RAMS Process,

— EN 50126-2:2017, Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Systems Approach to Safety.

This document is based on the system life cycle described in EN 50126-1:2017, EN 50126-2:2017 and is in line with the EN 61508 series. EN 50126-1:2017, EN 50126-2:2017, EN 50716:2023 and this document comprise the railway sector equivalent of the EN 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 EN 61508 series.

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

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 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 occupational health and safety of personnel or potential threats created by the technology regardless of their intended functions (e.g. presence of sharp edges, presence of electric voltage, presence of combustible material). Cybersecurity aspects of functional safety are addressed only to the extent consistent with the application of the relevant standards, where needed.

This document applies to all the phases of the life cycle of a safety-related electronic system, focusing in particular on phases from 4 (specification of system requirements) to 10 (system acceptance) as defined in EN 50126-1:2017.

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

This document is not necessarily applicable to systems, subsystems or equipment which had already been accepted prior to the date of withdrawal (dow) of the standards conflicting with this document. However, so far as reasonably practicable, it is applicable to modifications and extensions to such systems, subsystems and equipment.

NOTE In the case of partial modifications, it can happen that the system can no longer be declared compliant with a single version of the standard, meaning that the modified part will be compliant with the current version and the unmodified parts will be compliant with the previous version.

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, to the extent of 6.2, 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.

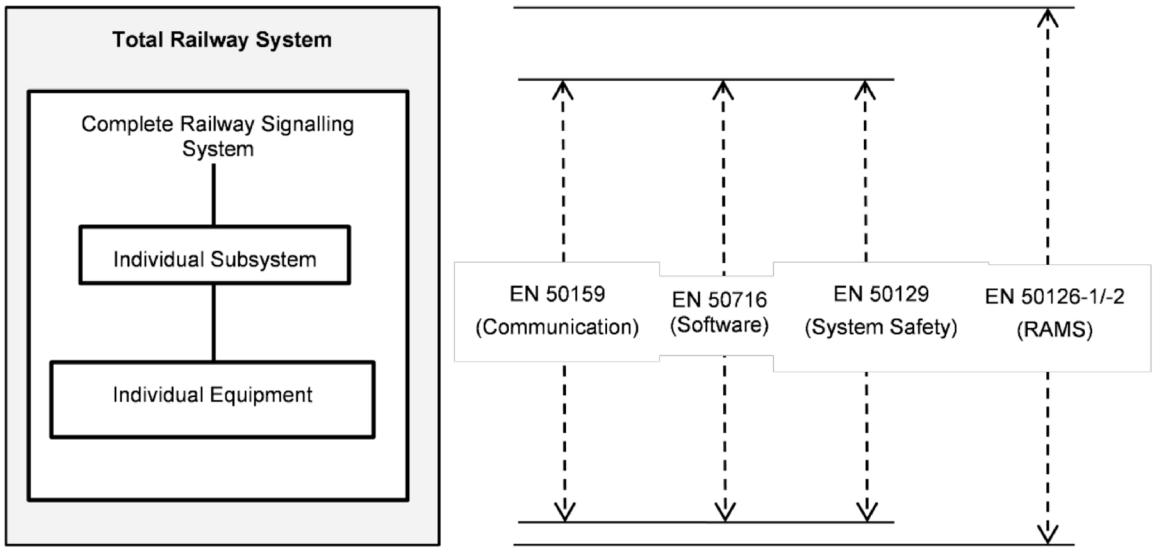


Figure 1 — Scope of the main CENELEC railway application standards

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

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.

EN 50124-1:2017, *Railway applications - Insulation coordination - Part 1: Basic requirements - Clearances and creepage distances for all electrical and electronic equipment*

EN 50125-1:2014, *Railway applications - Environmental conditions for equipment - Part 1: Rolling stock and on-board equipment*

EN 50125-3:2003,[1] *Railway applications - Environmental conditions for equipment - Part 3: Equipment for signalling and telecommunications*

EN 50126-1:2017,[2] *Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process*

EN 50126-2:2017,[3] *Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety*

EN 50159:2010,[4] *Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems*

EN 50716:2023, *Railway Applications - Requirements for software development*

EN IEC 60664-1:2020,[5] *Insulation coordination for equipment within low-voltage supply systems - Part 1: Principles, requirements and tests (IEC 60664-1:2020)*

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:

— ISO Online browsing platform: available at https://www.iso.org/obp/

— IEC Electropedia: available at https://www.electropedia.org/

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”.]

[1] As impacted by EN 50125-3/2003/corrigendum May 2010.
[2] As impacted by EN 50126-1:2017/A1:2024.
[3] As impacted by EN 50126-2:2017/A1:2024.
[4] As impacted by EN 50159:2010/A1:2020.
[5] As impacted by EN IEC 60664-1:2020/AC:2020-12 and EN IEC 60664-1:2020/A1:2025.

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

3.1.2
audit
systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled

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

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

3.1.3
basic insulation
insulation that provides basic protection

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

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

3.1.4
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 EN 50126-2:2017, no additional requirements are defined in this document.

[SOURCE: EN 50126-1:2017, 3.7, modified – Note 1 to entry has been added.]

3.1.5
causal analysis
analysis of the reasons how and why a particular hazard can come into existence

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

3.1.6
common cause failures
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.]

3.1.7
configuration
structuring and interconnection of the hardware and software of a system for its intended application

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

3.1.8
consequence analysis
analysis of events which are likely to happen after a hazard has occurred

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

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

3.1.9
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]

3.1.10
cybersecurity
actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, or damage to systems or informational assets

Note 1 to entry: Cybersecurity includes the concepts of identification, authentication, accountability, authorization, availability, and privacy.

Note 2 to entry: It is recognized that the term “cybersecurity” has a broader meaning in other standards and guidance, often including non-malevolent threats, human errors, and protection against natural disasters. Those aspects, except human errors degrading security controls, are not included in this document.

3.1.11
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)

3.1.12
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”.]

3.1.13
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.]

3.1.14
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 to entry, for definition of rated insulation voltage and rated impulse voltage, see EN 50124-1:2017. Similar definitions can also be found in EN IEC 60664-1:2020.

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

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

3.1.15
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.]

3.1.16
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]

3.1.17
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.]

3.1.18
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]

3.1.19
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, can 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, can 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 – “may” has been changed to “can” in notes to entry 1 and 2. Note 3 to entry has been added.]

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

3.1.20
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]

3.1.21
fault
<in a system> abnormal condition that could lead to an error in a system

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

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

3.1.22
fault detection time
time interval between failure and detection of the resulting fault

[SOURCE: IEC 60050-192:2024, 192-07-11, modified – The deprecated term “undetected fault time” as well as Figures 1 and 2 have been deleted.]

3.1.23
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.

3.1.24
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.]

3.1.25
harm
injury or damage to the health of people, or damage to property or the environment

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

3.1.26
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”.

Note 2 to entry: This means that there is at least one scenario in which the hazard, under credible circumstances, leads to an accident.

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

3.1.27
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]

3.1.28
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]

3.1.29
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”.]

3.1.30
independence of roles
freedom from involvement in the same intellectual, commercial or management entity

3.1.31
independent safety assessment
process to determine whether a system or product meets the specified safety requirements and to form a judgement as to whether the product is fit for its intended purpose in relation to safety

[SOURCE: EN 50126-1:2017, 3.33, modified – “the system/product” has been changed to “a system or product”. Note 1 to entry has been deleted.]

3.1.32
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]

3.1.33
negation
enforcement of a safe state following detection of a hazardous fault

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

3.1.34
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]

3.1.35
pre-existing item
item that already exists and that was not developed specifically for the current project

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

3.1.36
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”.]

3.1.37
railway duty holder
body with the overall accountability for operating a railway system within the legal framework

Note 1 to entry: Railway duty holder accountabilities for the overall system or its parts and life cycle activities are sometimes split between one or more bodies or entities. For example:

— the owner(s) of one or more parts of the system assets and their purchasing agents;

— the operator of the system;

— the maintainer(s) of one or more parts of the system.

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

[SOURCE: EN 50126-1:2017, 3.48]

3.1.38
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.]

3.1.39
random fault
unpredictable occurrence of a fault

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

3.1.40
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.]

3.1.41
reinforced insulation
insulation that provides a degree of protection against electric shock equivalent to double insulation

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

[SOURCE: IEC 60050-195:2021, 195-06-09]

3.1.42
reliability
<of an item> ability to perform as required, without failure, for a given time interval, under given conditions

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

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]

3.1.43
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]

3.1.44
risk
<for railway safety> combination of the frequency of occurrence of harm and the severity of that harm

[SOURCE: IEC 60050-351:2013, 351-57-03, modified — “probability” has been replaced with “frequency”.]

3.1.45
safe state
condition which continues to preserve safety

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

3.1.46
safety
freedom from unacceptable risk

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

3.1.47
safety acceptance
safety status given to a product by the final user

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

3.1.48
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]

3.1.49
safety authority
body responsible for delivering the authorization for the operation of the safety-related system

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

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

3.1.50
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]

3.1.51
safety function
<in railway> function whose sole purpose is to ensure safety

Note 1 to entry: All safety functions are safety-related, 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: EN 50126−1:2017, 3.68, modified – Note 1 to entry has been simplified and “may” has been changed to “can” in note 2 to entry.]

3.1.52
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”.]

3.1.53
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. For further explanations on SIL misuse, refer to EN 50126-2:2017, 10.2.12.

[SOURCE: IEC 60050-821:2017, 821-11-46, modified – “number which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures” has been replaced with “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”. Notes 1 and 2 to entry have been added]

3.1.54
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]

3.1.55
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]

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

3.1.56
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]

3.1.57
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.]

3.1.58
signalling system
<railway> 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.]

3.1.59
solid insulation
solid insulating material, or a combination of solid insulating materials, placed between two conductive parts or between a conductive part and a body part

EXAMPLE In the case of a printed board with a coating, solid insulation consists of the board itself as well as the coating. In other cases, solid insulation consists of the encapsulating material

[SOURCE: IEC 60050-903:2013, 903-04-14]

3.1.60
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]

3.1.61
subsystem
part of a system, which is itself a system

[SOURCE: IEC 60050-192:2015, 192-01-04, modified – Note 1 to entry has been omitted.]

3.1.62
supplementary insulation
independent insulation applied in addition to basic insulation, that provides fault protection

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

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

3.1.63
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.]

3.1.64
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]

3.1.65
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 — “unidentified hazardous errors and the causes thereof” has been replaced with “hazardous systematic faults” and Note 1 to entry has been added.]

3.1.66
systematic fault,
<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]

3.1.67
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.]

3.1.68
tolerable risk
risk which is accepted in a given context based on the applicable legal framework

Note 1 to entry: This definition also applies to “tolerable hazard” and “tolerable hazard rate”. In this standard tolerable and acceptable are considered as synonymous when associated to hazard or risk.

[SOURCE: IEC Guide 116:2010, 3.14, modified — “current values of society” has been replaced by “applicable legal framework”; Note 1 to entry has been added.]

3.1.69
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.

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

Note 3 to entry: In design and implementation, 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 60050-192:2024, 192-01-18, modified – Note 1 to entry has been modified. Notes 3 and 4 to entry have been added.]

3.1.70
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 60050-192:2024, 192-01-17, modified – Notes 1, 2 and 3 to entry has been modified.]

3.2 Abbreviated terms

For the purposes of this document, the following abbreviations apply:

CCF Common Cause Failures
COTS Commercial Off The Shelf
CPLD Complex Programmable Logic Device
DC Direct Current
DES Designer
DT Down Time, $T_D + T_N + T_R$
EMC ElectroMagnetic Compatibility
EMI ElectroMagnetic Interference
EPLD Erasable Programmable Logic Device
ESD ElectroStatic Discharge
FFR Functional Failure Rate
FMEA Failure Modes and Effects Analysis
FPGA Field-Programmable Gate Array
FR Failure Rate
FTA Fault Tree Analysis
GA Generic Application
GASC Generic Application Safety Case
GP Generic Product
GPSC Generic Product Safety Case
HAZOP HAZard and OPerability study
HDL Hardware Description Language
HW Hardware

This is a preview of DS/EN 50129:2026. Click here to purchase the full version from the ANSI store.

IP	Intellectual Property
ISA	Independent Safety Assessor
LCA	Logic Cell Array
MTBF	Mean Time Between Failure
PAL	Programmable Array Logic
PLA	Programmable Logic Array
PLD	Programmable Logic Device
PM	Project Manager
RAMS	Reliability, Availability, Maintainability and Safety
RMS	Root Mean Square
SA	Specific Application
SASC	Specific Application Safety Case
SDR	Safe Down Rate, inverse of SDT
SDT	Safe Down Time, $T_D + T_N$
SIL	Safety Integrity Level
SRAC	Safety-Related Application Condition
SW	Software
TFFR	Tolerable Functional (unsafe) Failure Rate
THR	Tolerable Hazard Rate
T_D	Detection time, interval between failure and fault detection
T_N	Negation time, interval between fault detection and fault negation
T_R	Repair time, interval between fault negation and fault repair
UPIC	User Programmable Integrated Circuit