SLOVENSKI STANDARD
oSIST prEN 50129:2025

01-januar-2025

Železniške naprave - Komunikacijski, signalni in procesni sistemi - Signalno-varnostni elektronski sistemi

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

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

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

Ta slovenski standard je istoveten z: **prEN 50129:2024**

ICS:

35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport
45.020	Železniška tehnika na splošno	Railway engineering in general

oSIST prEN 50129:2025 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 50129

November 2024

ICS

Will supersede 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 télécommunication et de traitement - Systèmes électroniques de sécurité pour la signalisation

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

This draft European Standard is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2025-02-07.

It has been drawn up by CLC/SC 9XA.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CENELEC 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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

Contents

Page

European foreword

This document (prEN 50129:2024) has been prepared by CLC/SC 9XA “Communication, signalling and processing systems” of CLC/TC 9X “Electrical and electronic applications for railways”.

This document is currently submitted to the Enquiry.

The following dates are proposed:

• latest date by which the existence of this document has to be announced at national level	(doa)	dor + 6 months
• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	dor + 12 months
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	dor + 36 months (to be confirmed or modified when voting)

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

prEN 50129:2024 includes the following significant technical changes with respect to EN 50129:2018.

— A better alignment with the rules given in the CEN-CENELEC Internal Regulation Part 3 has been made;

— requirements and guidance have been added on the following topics:

  o reuse of pre-existing systems,

  o safety-related tools,

  o relationship between cybersecurity and safety,

  o safety qualification tests,

  o basic integrity,

  o insulation coordination.

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

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. For safety-related systems which include software, additional conditions are defined in EN 50716:2023.

Additional requirements for safety-related communication are defined in EN 50159:2010.

This document does not specify the cybersecurity requirements for the development, implementation, maintenance and operation of security policies, services, or systems where needed, since cyberattacks can affect also the functional safety of a system. 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 necessary. 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 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 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, EN 50126-2 and is in line with the EN 61508 series. EN 50126-1 / EN 50126-2 / EN 50716 / EN 50129 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.

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 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 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 5 (architecture and apportionment 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 this document. However, so far as reasonably practicable, it is applicable to modifications and extensions to such 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, 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.

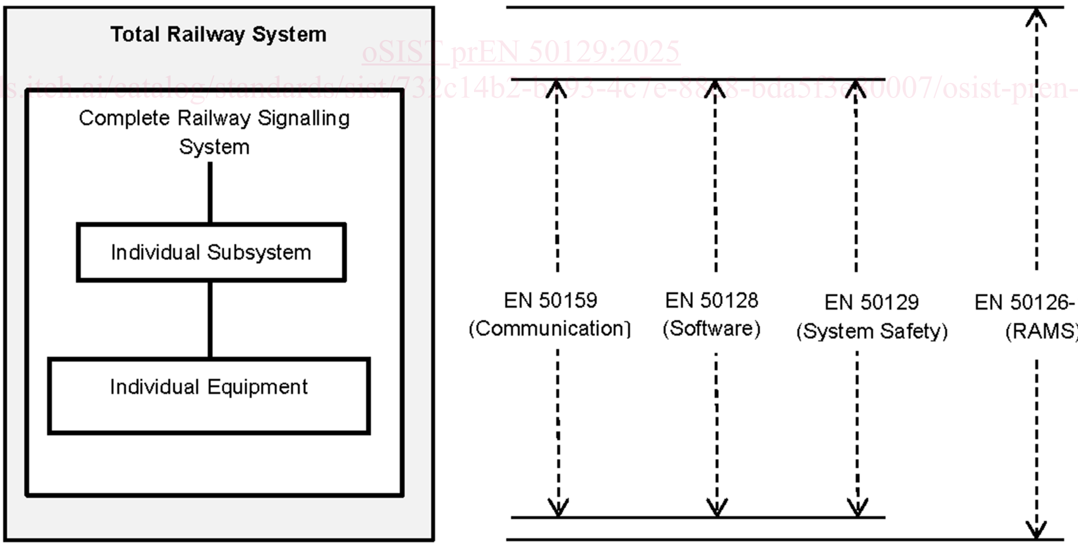

Figure 1 — Scope of the main CENELEC railway application standards

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

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

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*

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

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

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”]

3.1.2
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]

3.1.3
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 EN 50126-2:2017, no additional requirements are defined in this document.

[SOURCE: EN 50126-1:2017, 3.7, modified – “equal to, or” has been added; 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
cybersecurity, <in railway application>
set of activities and measures taken with the objective to prevent, detect, and react to unauthorized access or cyberattack which could lead to an accident, an unsafe situation, or railway application performance degradation

Note 1 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.

[SOURCE: CLC/TS 50701:2023, 3.1.32]

3.1.10
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)

3.1.11
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”.]

3.1.12
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.]

3.1.13
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 60664-1:2020.

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

3.1.14
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.]

3.1.15
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]

3.1.16
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.]

3.1.17
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]

3.1.18
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.]

3.1.19
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]

3.1.20
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]

3.1.21
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.]

3.1.22
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.

3.1.23
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.]

3.1.24
harm
injury or damage to the health of people, or damage to property or the environment

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

3.1.25
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.

3.1.26
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]

3.1.27
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]