NSAI Standards

Irish Standard
I.S. EN 50129:2018

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

I.S. EN 50129:2018

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:	*Published:*
EN 50129:2018	2018-11-23

This document was published under the authority of the NSAI and comes into effect on:	ICS number:
2018-12-11	93.100
	NOTE: If blank see CEN/CENELEC cover page

NSAI	T +353 1 807 3800	Sales:
1 Swift Square,	F +353 1 807 3838	T +353 1 857 6730
Northwood, Santry	E standards@nsai.ie	F +353 1 857 6729
Dublin 9	W NSAI.ie	W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

National Foreword

I.S. EN 50129:2018 is the adopted Irish version of the European Document EN 50129:2018, Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

For relationships with other publications refer to the NSAI web store.

Compliance with this document does not of itself confer immunity from legal obligations.

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.

This page is intentionally left blank

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50129

November 2018

ICS 93.100

Supersedes CLC/TR 50451:2007, CLC/TR 50506-1:2007, CLC/TR 50506-2:2009, EN 50129:2003

English Version

Railway applications - Communication, signalling and processing systems - 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 - Sicherheitsrelevante elektronische Systeme für Signaltechnik

This European Standard was approved by CENELEC on 2018-06-07. 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey 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

Ref. No. EN 50129:2018 E

Contents **Page**

European foreword

This document (EN 50129:2018) 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)	2019-05-23
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2021-11-23

This document supersedes EN 50129:2003.

CLC/TR 50451:2007, CLC/TR 50506-1:2007 and CLC/TR 50506-2:2009 are withdrawn by the time the present Publication is published.

The significant technical changes with respect to EN 50129:2003 are the following:

— A better alignment with the life cycle phases described in EN 50126-1:2017 has been made;

  — Clause 5 describes the requirements that apply to the development of safety-related electronic systems (until phase 9 of the life cycle),

  — Clause 8 focuses on the requirements for safety acceptance and approval of safety-related electronic systems and subsequent phases;

— Requirements and guidance have been added in Clause 6 on the following topics:

  — reuse of pre-existing systems,

  — safety-related tools,

  — impact of IT security threats on functional safety,

  — specific application safety cases;

— Requirements for the structure and content of the safety case are now defined in a dedicated Clause 7;

— Annex A has been aligned with EN 50126-2:2017 for the specification and allocation of safety integrity requirements;

— The content of former Annex D has been merged with Annex B, and has been changed from informative to normative;

— The status of the Annex E has been changed from informative to normative;

— An Annex F has been added as an informative annex on User Programmable Integrated Circuits.

A more detailed comparison of changes between EN 50129:2003 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.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

For the relationship with EU Directive(s) see informative Annex ZZ, which is an integral part of this document.

The structure of this document is described in Clause 4.

This document is intended to be used in conjunction with 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*", and EN 50128:2011, "*Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems*".

This document has been prepared under the Mandate M/483 given to CENELEC by the European Commission and the Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method (CSM) for risk evaluation and assessment and repealing Regulation (EC) No 352/2009 (with the subsequent amendment, Commission Implementing Regulation (EU) No 2015/1136 of 13 July 2015).

Introduction

This document defines requirements for the acceptance of safety-related electronic systems in the railway signalling field.

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, since this can vary in different circumstances.

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, see EN 50128; for safety-related data communication, see EN 50159.

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

This document is in line with, and uses relevant sections of:

— 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 50128, EN 50129 comprise the railway sector equivalent of the EN 61508 series so far as Railway Communication, Signalling and Processing Systems are concerned. When compliance with these documents has been demonstrated, further evaluation of compliance with the EN 61508 series is not required.

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 is not intended to 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.

This document applies to all the phases of the life cycle of a safety-related electronic system, focusing in particular on phases from 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 applicable to existing systems, subsystems or equipment which had already been accepted prior to the creation of this document. However, so far as reasonably practicable, it should be applied 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 should also be applied, 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. As a minimum, evidence should be provided in such cases (more information is given in 6.2) to demonstrate either

– that the equipment is not relied on for safety, or

– that the equipment can be relied on for those functions which relate to safety.

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.

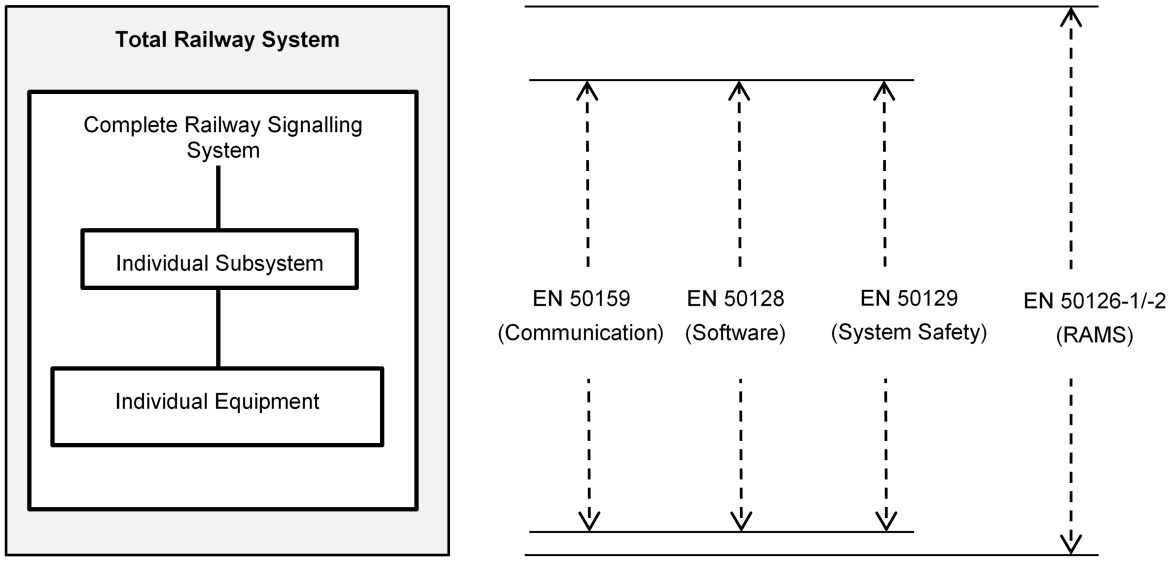

Figure 1 — Scope of the main CENELEC railway application standards

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

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

EN 50125-3, *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 50128, *Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems*

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

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

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

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

3.1.1
accident
unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage

[SOURCE: IEC 60050-821:2017, 821-12-02]

3.1.2
basic integrity
integrity attribute for safety-related functions with a TFFR higher than (less demanding) 10^{-5} h^{-1} or for non-safety-related functions

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 – The note 1 to entry has been added.]

3.1.3
causal analysis
analysis of the reasons how and why a particular hazard can come into existence

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

3.1.4
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]

3.1.5
configuration
structuring and interconnection of the hardware and software of a system for its intended application

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

3.1.6
consequence analysis
analysis of events which are likely to happen after a hazard has occurred

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

3.1.7
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]

3.1.8
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 by “solutions”.]

3.1.9
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 failure. 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]

3.1.10
DC fault model
fault category that includes the following failure modes: stuck-at faults, stuck-open, open or high impedance outputs as well as short circuits between signal lines, and for integrated circuits, short circuit between any two connections (pins)

3.1.11
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 – “hardware component” has been added as a synonym.]

3.1.12
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]

3.1.13
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]

3.1.14
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]

3.1.15
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 – The note 3 to entry has been added.]