This is a preview of "DS/EN 50129:2018". Click here to purchase the full version from the ANSI store.

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

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

DANSK STANDARD
Danish Standards Association

Göteborg Plads 1
DK-2150 Nordhavn

Tel: +45 39 96 61 01
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 50129:2018". Click here to purchase the full version from the ANSI store.

DS projekt: M310451
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 50129:2018

DS-publikationen er på engelsk.

Denne publikation erstatter: DS/EN 50129 + AC:2010, DS/CLC/TR 50451:2007, DS/CLC/TR 50506-1:2007, DS/CLC/TR 50506-2:2010

DS-publikationstyper
Dansk Standard udgiver forskellige publikationstyper.
Typen på denne publikation fremgår af forsiden.

Der kan være tale om:

Dansk standard
- standard, der er udarbejdet på nationalt niveau, eller som er baseret på et andet lands nationale standard, eller
- standard, der er udarbejdet på internationalt og/eller europæisk niveau, og som har fået status som dansk standard

DS-information
- publikation, der er udarbejdet på nationalt niveau, og som ikke har opnået status som standard, eller
- publikation, der er udarbejdet på internationalt og/eller europæisk niveau, og som ikke har fået status som standard, fx en teknisk rapport, eller
- europæisk præstandard

DS-håndbog
- samling af standarder, eventuelt suppleret med informativt materiale

DS-hæfte
- publikation med informativt materiale

Til disse publikationstyper kan endvidere udgives
- tillæg og rettelsesblade

DS-publikationsform
Publikationstyperne udgives i forskellig form som henholdsvis
- fuldtekstpublikation (publikationen er trykt i sin helhed)
- godkendelsesblad (publipukationen leveres i kopi med et trykt DS-omslag)
- elektronisk (publikationen leveres på et elektronisk medie)

DS-betegnelse
Alle DS-publikationers betegnelse begynder med DS efterfulgt af et eller flere præfikser og et nr., fx **DS 383**, **DS/EN 5414** osv. Hvis der efter nr. er angivet et **A** eller **Cor**, betyder det, enten at det er et **tillæg** eller et **rettelsesblad** til hovedstandarden, eller at det er indført i hovedstandarden.
DS-betegnelse angives på forsiden.

Overensstemmelse med anden publikation:
Overensstemmelse kan enten være IDT, EQV, NEQ eller MOD
- **IDT:** Når publikationen er identisk med en given publikation.
- **EQV:** Når publikationen teknisk er i overensstemmelse med en given publikation, men præsentationen er ændret.
- **NEQ:** Når publikationen teknisk eller præsentationsmæssigt ikke er i overensstemmelse med en given standard, men udarbejdet på baggrund af denne.
- **MOD:** Når publikationen er modificeret i forhold til en given publikation.

EUROPEAN STANDARD EN 50129

This is a preview of "DS/EN 50129:2018". Click here to purchase the full version from the ANSI store.

EUROPÄISCHE NORM

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

© 2018 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN 50129:2018 E

This is a preview of "DS/EN 50129:2018". Click here to purchase the full version from the ANSI store.

Contents **Page**

European foreword **5**
Introduction **7**
1 Scope **8**
2 Normative references **9**
3 Terms, definitions and abbreviations **10**
3.1 Terms and definitions 10
3.2 Abbreviations 20
4 Overall framework of this standard **21**
5 Requirements for developing safety-related electronic systems **22**
5.1 Introduction 22
5.2 The quality management process 23
5.3 The safety management process 26
6 Requirements for elements following different life cycles **36**
6.1 Introduction 36
6.2 Use of pre-existing items 36
6.3 Safety-related tools for electronic systems 39
6.4 Physical security and IT-Security 41
7 The Safety Case: structure and content **42**
7.1 The Safety Case structure 42
7.2 The Technical Safety Report 44
7.3 Generic and Specific Safety Cases 55
7.4 Provisions for the Specific Application Safety Case 55
7.5 Dependencies between Safety Cases 56
8 System safety acceptance and subsequent phases **57**
8.1 System safety acceptance process 57
8.2 Operation, maintenance and performance monitoring 61
8.3 Modification and retrofit 61
8.4 Decommissioning and disposal 61
Annex A (normative) **Safety Integrity Levels** **62**
A.1 Introduction **62**
A.2 Safety requirements **62**
A.3 Safety integrity **63**
A.4 Determination of safety integrity requirements **64**
A.4.1 General 64
A.4.2 Risk Assessment 65
A.4.3 Hazard Control 67

This is a preview of "DS/EN 50129:2018". Click here to purchase the full version from the ANSI store.

A.4.4 Identification and treatment of new hazards arising from design 72
A.5 Allocation of SILs 73
A.5.1 General aspects 73
A.5.2 Relationship between SIL and associated TFFR 74
Annex B (normative) **Management of faults for safety-related functions 77**
B.1 Introduction 77
B.2 General concepts 78
B.2.1 Detection and negation times 78
B.2.2 Composition of two independent items 79
B.3 Effects of faults 80
B.3.1 Effects of single faults 80
B.3.2 Influences between items 81
B.3.3 Detection of single faults 87
B.3.4 Action following detection (retention of safe state) 90
B.3.5 Effects of multiple faults 92
B.3.6 Defence against systematic faults 95
Annex C (normative) **Identification of hardware component failure modes 96**
C.1 Introduction 96
C.2 General procedure 96
C.3 Procedure for integrated circuits 96
C.4 Procedure for components with inherent physical properties 97
C.5 General provisions concerning component failure modes 97
Annex D (informative) **Example of THR/TFFR/FR apportionment and SIL allocation 117**
Annex E (normative) **Techniques and measures for the avoidance of systematic faults and the control of random and systematic faults 119**
E.1 Introduction 119
E.2 Tables of techniques and measures 121
Annex F (informative) Guidance on User Programmable Integrated Circuits 130
F.1 Introduction 130
F.1.1 Purpose 130
F.1.2 Terminology and context 131
F.2 UPIC life cycle 132
F.2.1 Organization, roles, responsibilities and personnel competencies 134
F.2.2 UPIC Requirements 134
F.2.3 UPIC Architecture and Design 135
F.2.4 Logic Component Design 136
F.2.5 Logic Component Coding 136
F.2.6 Logic Component Verification 136

This is a preview of "DS/EN 50129:2018". Click here to purchase the full version from the ANSI store.

F.2.7 UPIC Physical Implementation 136
F.2.8 UPIC Integration 136
F.2.9 UPIC Validation 136
F.2.10 Requirements for use of pre-existing logic components 136
F.3 Detailed technical requirements for UPIC 136
F.3.1 Guidance on safety architecture 136
F.3.2 Protection against random faults – architectural principles 137
F.3.3 Protection against systematic faults – (techniques/measures) 137
Annex G (informative) **Changes at this document compared to EN 50129:2003 ..... 147**
Annex ZZ (informative) **Relationship between this document and the Essential Requirements of EU Directive 2008/57/EC 151**
Bibliography 153

This is a preview of "DS/EN 50129:2018". Click here to purchase the full version from the ANSI store.

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).

This is a preview of "DS/EN 50129:2018". Click here to purchase the full version from the ANSI store.

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).

This is a preview of "DS/EN 50129:2018". Click here to purchase the full version from the ANSI store.

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.

This is a preview of "DS/EN 50129:2018". 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 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.

This is a preview of "DS/EN 50129:2018". Click here to purchase the full version from the ANSI store.

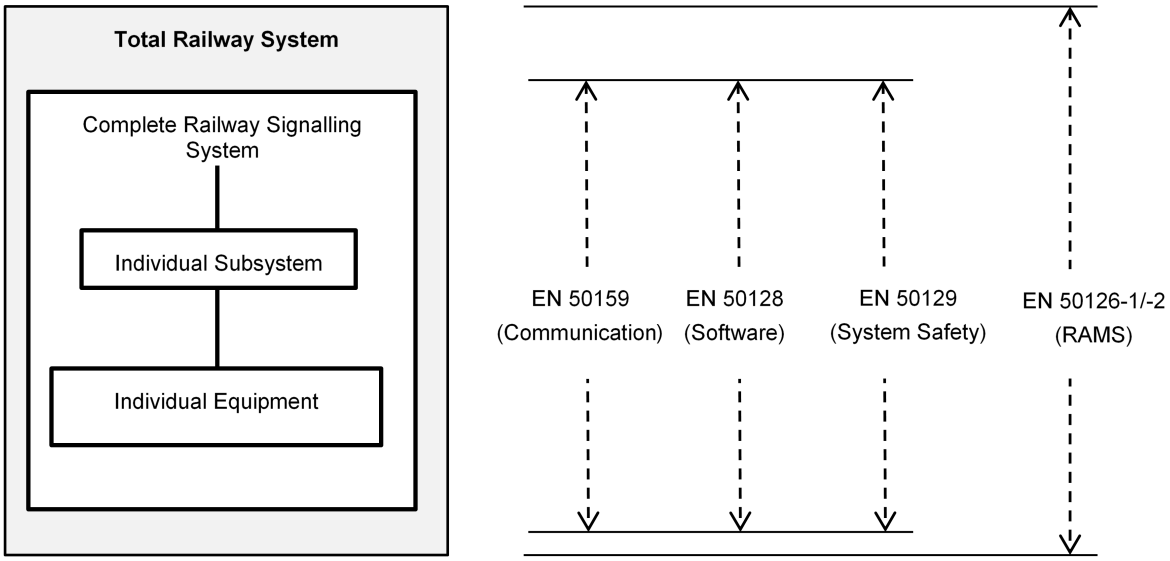


Figure 1 — Scope of the main CENELEC railway application standards

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)*