SLOVENSKI STANDARD
SIST EN 50129:2003

01-maj-2003

Nadomeġ ļa:
SIST ENV 50129:1998

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

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

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

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

Ta slovenski standard je istoveten z: **EN 50129:2003**

ICS:

35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade
45.020	Železniška tehnika na splošno	Railway engineering in general

SIST EN 50129:2003 **en**

EUROPEAN STANDARD **EN 50129**

NORME EUROPÉENNE

EUROPÄISCHE NORM February 2003

ICS 93.100 Supersedes ENV 50129:1998

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 2002-12-01. 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 Central Secretariat 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 Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and United Kingdom.

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

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Ref. No. EN 50129:2003 E

Foreword

This European Standard was prepared by SC 9XA, Communication, signalling and processing systems, of Technical Committee CENELEC TC 9X, Electrical and electronic applications for railways.

The text of the draft was submitted to the formal vote and was approved by CENELEC as EN 50129 on 2002-12-01.

This European Standard supersedes ENV 50129:1998.

This European Standard was prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and supports the essential requirements of Directive 96/48/EC.

The following dates were fixed:

- latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2003-12-01

- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2005-12-01

Annexes designated "normative" are part of the body of the standard.
Annexes designated "informative" are given for information only.
In this standard, Annexes A, B and C are normative and Annexes D and E are informative.

Contents

Introduction

This document is the first European Standard defining requirements for the acceptance and approval of safety-related electronic systems in the railway signalling field. Until now only some differing national recommendations and general advice of the UIC (International Union of Railways) on this topic were in existence.

Safety-related electronic systems for signalling include hardware and software aspects. To install complete safety-related systems, both parts within the whole life-cycle of the system have to be taken into account. The requirements for safety-related hardware and for the overall system are defined in this standard. Other requirements are defined in associated CENELEC standards.

The aim of European railway authorities and European railway industry is to develop compatible railway systems based on common standards. Therefore cross-acceptance of Safety Approvals for sub-systems and equipment by the different national railway authorities is necessary. This document is the common European base for safety acceptance and approval of electronic systems for railway signalling applications.

Cross-acceptance is aimed at generic approval, not specific applications. Public procurement within the European Community concerning safety-related electronic systems for railway signalling applications will in future refer to this standard when it becomes an EN.

The standard consists of the main part (Clause 1 to Clause 5) and Annexes A, B, C, D and E. The requirements defined in the main part of the standard and in Annexes A, B and C are normative, whilst Annexes D and E are informative.

This standard is in line with, and uses relevant sections of EN 50126: "Railway applications: The Specification and Demonstration of Dependability - Reliability, Availability, Maintainability and Safety (RAMS)". This standard and EN 50126 are based on the system life-cycle and are in line with EN 61508-1, which is replaced by the set of EN 50126/EN 50128/EN 50129, as far as Railway Communication, Signalling and Processing Systems are involved. Meeting the requirements in these standards is sufficient to ensure that further compliance to EN 61508-1 need not be evaluated.

Because this standard is concerned with the evidence to be presented for the acceptance of safety-related systems, it specifies those life-cycle activities which shall be completed before the acceptance stage, followed by additional planned activities to be carried out after the acceptance stage. Safety justification for the whole of the life-cycle is therefore required.

This standard is concerned with what evidence is to be presented. Except where considered appropriate, it does not specify who should carry out the necessary work, since this may vary in different circumstances.

For safety-related systems which include programmable electronics, additional conditions for the software are defined in EN 50128.

Additional requirements for safety-related data communication are defined in EN 50159-1 and EN 50159-2.

1 Scope

This standard is applicable to safety-related electronic systems (including sub-systems and equipment) for railway signalling applications.

The scope of this standard, and its relationship with other CENELEC standards, are shown in Figure 1.

This standard is intended to apply to all safety-related railway signalling systems/sub-system/equipment. However, the hazard analysis and risk assessment processes defined in EN 50126 and this standard are necessary for all railway signalling systems/sub-systems/equipment, in order to identify any safety requirements. If analysis reveals that no safety requirements exist (i.e.: that the situation is non-safety-related), and provided the conclusion is not revised as a consequence of later changes, this safety standard ceases to be applicable.

This standard applies to the specification, design, construction, installation, acceptance, operation, maintenance and modification/extension phases of complete signalling systems, and also to individual sub-systems and equipment within the complete system. Annex C includes procedures relating to electronic hardware components.

This standard applies to generic sub-systems and equipment (both application-independent and those intended for a particular class of application), and also to systems/sub-systems/equipment for specific applications.

This standard is not applicable to existing systems/sub-systems/equipment (i.e. those which had already been accepted prior to the creation of this standard). However, as far as reasonably practicable, this standard should be applied to modifications and extensions to existing systems, sub-systems and equipment.

This standard is primarily applicable to systems/sub-systems/equipment which have been specifically designed and manufactured for railway signalling applications. It should also be applied, as far as reasonably practicable, to general-purpose or industrial equipment (e.g.: power supplies, modems, etc.), which is procured for use as part of a safety-related signalling system. As a minimum, evidence shall be provided in such cases 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 standard is applicable to the functional safety of railway signalling systems. It is not intended to deal with the occupational health and safety of personnel; this subject is covered by other standards.

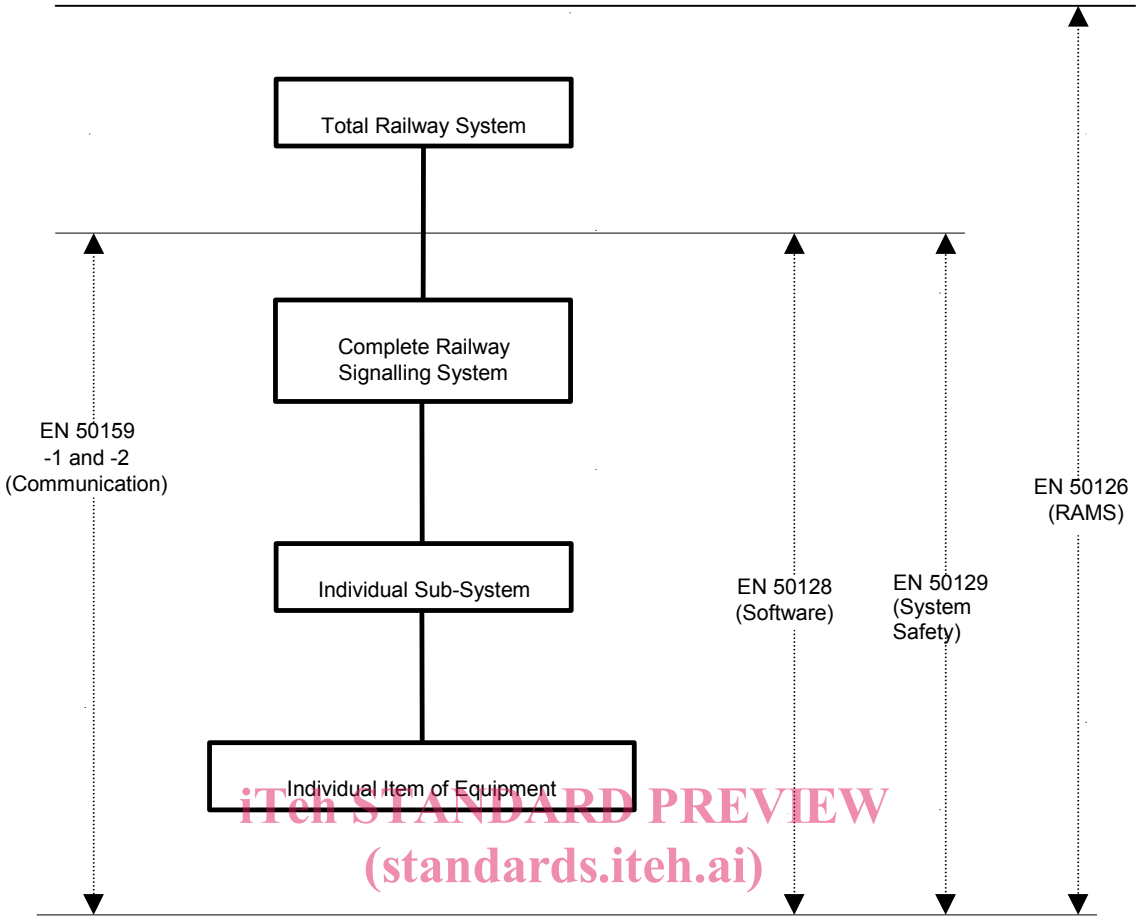

Figure 1 – Scope of the main CENELEC railway application standards

2 Normative references

This European Standard incorporates, by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

NOTE Additional informative references are included in Bibliography.

EN 50121 Series	Railway applications – Electromagnetic compatibility
EN 50124-1	Railway applications – Insulation coordination – Part 1: Basic requirements - Clearances and creepage distances for all electrical and electronic equipment
EN 50124-2	Railway applications – Insulation coordination – Part 2: Overvoltages and related protection
EN 50125-1	Railway applications – Environmental conditions for equipment – Part 1: Equipment on board rolling stock
EN 50125-3	Railway applications – Environmental conditions for equipment – Part 3: Equipment for signalling and communications
EN 50126	Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

EN 50128	Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems
EN 50155	Railway applications – Electronic equipment used on rolling stock
EN 50159-1	Railway applications – Communication, signalling and processing systems Part 1: Safety-related communication in closed transmission systems
EN 50159-2	Railway applications – Communication, signalling and processing systems Part 2: Safety related communication in open transmission systems
EN 61508-1	Functional safety of electrical/electronic/ programmable electronic safety-related systems - Part 1: General requirements (IEC 61508-1)
IEC 60664 Series	Insulation coordination for equipment within low-voltage systems

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this standard, the following definitions apply:

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

3.1.2
assessment
the process of analysis to determine whether the design authority and the validator have achieved a product that meets the specified requirements and to form a judgement as to whether the product is fit for its intended purpose

3.1.3
authorisation
the formal permission to use a product within specified application constraints

3.1.4
availability
the ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided

3.1.5
can
is possible

3.1.6
causal analysis
analysis of the reasons how and why a particular hazard may come into existence

3.1.7
common-cause failure
failure common to items which are intended to be independent

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

3.1.9
configuration
the structuring and interconnection of the hardware and software of a system for its intended application

3.1.10
cross-acceptance
the status achieved by a product that has been accepted by one authority to the relevant European Standards and is acceptable to other authorities without the necessity for further assessment

3.1.11
design
the activity applied in order to analyse and transform specified requirements into acceptable design solutions which have the required safety integrity

3.1.12
design authority
the body responsible for the formulation of a design solution to fulfil the specified requirements and for overseeing the subsequent development and setting-to-work of a system in its intended environment

3.1.13
diversity
a means of achieving all or part of the specified requirements in more than one independent and dissimilar manner

3.1.14
equipment
a functional physical item

3.1.15
error
a deviation from the intended design which could result in unintended system behaviour or failure

3.1.16
fail-safe
a concept which is incorporated into the design of a product such that, in the event of a failure, it enters or remains in a safe state

3.1.17
failure
a deviation from the specified performance of a system. A failure is the consequence of a fault or error in the system

3.1.18
fault
an abnormal condition that could lead to an error in a system. A fault can be random or systematic

3.1.19
fault detection time
time span which begins at the instant when a fault occurs and ends when the existence of the fault is detected

3.1.20
function
a mode of action or activity by which a product fulfils its purpose

3.1.21
hazard
a condition that could lead to an accident

3.1.22
hazard analysis
the 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

3.1.23
hazard log
the document in which all safety management activities, hazards identified, decisions made and solutions adopted, are recorded or referenced

3.1.24
human error
a human action (mistake), which can result in unintended system behaviour/failure

3.1.25
implementation
the activity applied in order to transform the specified designs into their physical realisation

3.1.26
independence (functional)
freedom from any mechanism which can affect the correct operation of more than one function as a result of either systematic or random failure

3.1.27
independence (human)
freedom from involvement in the same intellectual, commercial and/or management entity

3.1.28
independence (physical)
freedom from any mechanism which can affect the correct operation of more than one system/sub-system/equipment as a result of random failures

3.1.29
individual risk
a risk which is related to a single individual only

3.1.30
maintainability
the probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources

3.1.31
maintenance
the combination of all technical and administrative actions, including supervision actions, intended to retain an item in, or restore it to, a state in which it can perform its required function

3.1.32
may
is permissible

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

3.1.34
negation time
time span which begins when the existence of a fault is detected and ends when a safe state is enforced

3.1.35
product
a collection of elements, interconnected to form a system/sub-system/equipment, in a manner which meets the specified requirements

3.1.36
quality
a user perception of the attributes of a product

3.1.37
railway authority
the body with the overall accountability to a safety authority for operating a safe railway system

3.1.38
random failure integrity
the degree to which a system is free from hazardous random faults

3.1.39
random fault
unpredictable occurrence of a fault

3.1.40
redundancy
the provision of one or more additional measures, usually identical, to provide fault tolerance

3.1.41
reliability
the ability of an item to perform a required function under given conditions for a given period of time

3.1.42
repair
measures for re-establishing the required state of a system/sub-system/equipment after a fault/failure

3.1.43
risk
the combination of the frequency, or probability, and the consequence of a specified hazardous event

3.1.44
safe state
a condition which continues to preserve safety

3.1.45
safety
freedom from unacceptable levels of risk of harm

3.1.46
safety acceptance
the safety status given to a product by the final user

3.1.47
safety approval
the safety status given to a product by the requisite authority when the product has fulfilled a set of pre-determined conditions

3.1.48
safety authority
the body responsible for delivering the authorisation for the operation of the safety related system

3.1.49
safety case
the documented demonstration that the product complies with the specified safety requirements

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

3.1.51
Safety Integrity Level
a number which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures

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

3.1.53
safety management
the management structure which ensures that the safety process is properly implemented

3.1.54
safety plan
the implementation details of how the safety requirements of the project will be achieved

3.1.55
safety process
the series of procedures that are followed to enable all safety requirements of a product to be identified and met

3.1.56
safety-related
carries responsibility for safety

3.1.57
shall
is mandatory

3.1.58
should
is recommended

3.1.59
signalling system
particular kind of system used on a railway to control and protect the operation of trains

3.1.60
stress profile
the degree and number of external influences which a product can withstand whilst performing its required functionality

3.1.61
sub-system
a portion of a system which fulfils a specialised function

3.1.62
system
a set of sub-systems which interact according to a design

3.1.63
systematic failure integrity
the degree to which a system is free from unidentified hazardous errors and the causes thereof

3.1.64
systematic fault
an inherent fault in the specification, design, construction, installation, operation or maintenance of a system, sub-system or equipment

3.1.65
system life-cycle
the series of activities occurring during a period of time that starts when a system is conceived and ends at decommissioning when the system is no longer available for use

3.1.66
technical safety report
documented technical evidence for the safety of the design of a system/sub-system/equipment

3.1.67
validation
the activity applied in order to demonstrate, by test and analysis, that the product meets in all respects its specified requirements

3.1.68
verification
the activity of determination, by analysis and test, at each phase of the life-cycle, that the requirements of the phase under consideration meet the output of the previous phase and that the output of the phase under consideration fulfils its requirements

3.2 Abbreviations

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

3.2.1	**AC**	alternating current
3.2.2	**ATP**	Automatic Train Protection
3.2.3	**CENELEC**	European Committee for Electrotechnical Standardisation