SLOVENSKI STANDARD
SIST ENV 50129:1998

01-november-1998

Railway applications - Safety related electronic systems for signalling

Railway applications - Safety related electronic systems for signalling

Bahnanwendungen - Sicherheitsrelevante elektronische Systeme für Signaltechnik

Applications ferroviaires - Systèmes électroniques de sécurité pour la signalisation

Ta slovenski standard je istoveten z: **ENV 50129:1998**

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 ENV 50129:1998 **en**

EUROPEAN PRESTANDARD

PRÉNORME EUROPÉENNE

EUROPÄISCHE VORNORM

ENV 50129

May 1998

Descriptors: Railway equipment, safety related systems, electronic components, safety integrity levels, safety requirements, safety acceptance, safety case

English version

Railway applications
Safety related electronic systems for signalling

Applications ferroviaires
Systèmes électroniques de sécurité pour la signalisation

Bahnanwendungen
Sicherheitsrelevante elektronische Systeme für Signaltechnik

This European Prestandard (ENV) was approved by CENELEC on 1997-06-17 as a prospective standard for provisional application. The period of validity of this ENV is limited initially to three years. After two years the members of CENELEC will be requested to submit their comments, particularly on the question whether the ENV can be converted into a European Standard (EN).

CENELEC members are required to announce the existence of this ENV in the same way as for an EN and to make the ENV available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the ENV) until the final decision about the possible conversion of the ENV into an EN is reached.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, 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. ENV 50129:1998 E

Foreword

This European Prestandard was prepared by Subcommittee 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 CENELEC members for comments and approved as ENV 50129 during the voting meeting of CENELEC/SC 9XA on 1997-06-17.

The following date was fixed:

- latest date by which the existence of the ENV has to be announced at national level (doa) 1998-02-01

Contents

Page

Annexes

Introduction

This document is the first European standardization document 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 subsystems 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 European Standard (EN)

The standard consists of the main part (clauses 1 to 6) and annexes A, B, C, D, E and F. The requirements defined in the main part of the standard and in annexes A, B and C are normative, whilst annexes D, E and F are informative.

This European Prestandard standard is consistent with, and uses relevant sections of EN 50126: "Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)". In particular, both standards are based on the system life-cycle

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 "Railway applications - Software for railway control and protection systems".

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

1 Scope

This European Prestandard is applicable to safety-related electronic systems (including subsystems and equipment) for railway signalling applications.

The scope of this European Prestandard, and its relationship with other CENELEC standards, are shown in figure 1.

This European Prestandard is primarily intended to apply to "fail-safe" and "high-integrity" systems (e.g.: main-line signalling and ATP systems), rather than medium or low-integrity systems (e.g.: running "on-sight", or in marshalling yards where points are moved as vehicles approach). However, in all cases the hazard analysis and risk assessment processes defined in EN 50126 are necessary, in order to identify the safety requirements for each particular situation. This includes those cases where the analysis and assessment reveal that no safety requirements exist; however, once this conclusion has been reached (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 European Prestandard applies to the acceptance of the specification, design, construction, installation, acceptance, operation, maintenance and modification/extension of complete systems, and also to individual subsystems and equipment within the complete system. Annex C includes procedures relating to electronic hardware components.

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

This European Prestandard is not applicable to existing systems/subsystems/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, subsystems and equipment.

This European Prestandard is primarily applicable to systems/subsystems/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 European Prestandard 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.

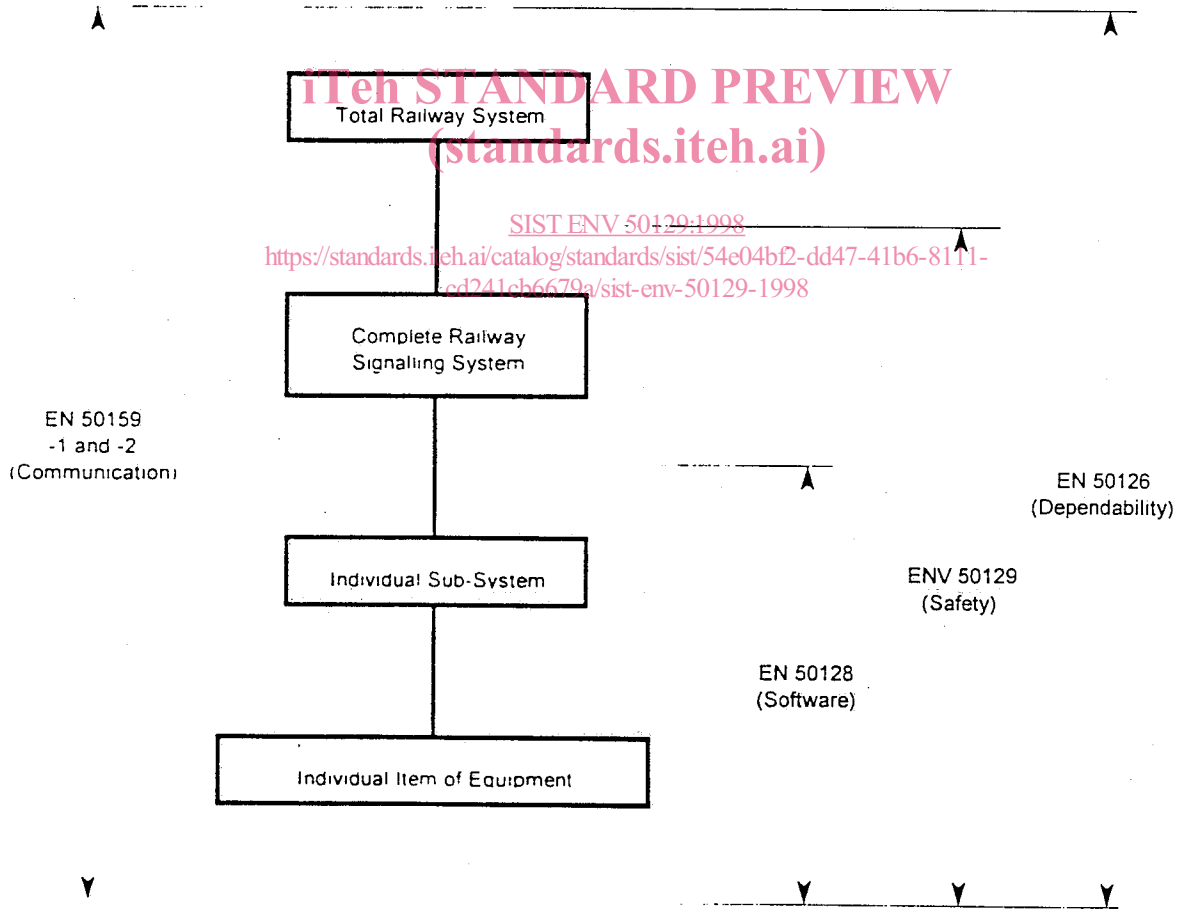

Figure 1: Scope of CENELEC railway standards

2 Normative references

This European Prestandard 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 Prestandard only when in corporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

NOTE: Additional informative references are included in annex F: Bibliography.

EN 50121-2	Railway applications - Electromagnetic compatibility (EMC) - Interaction of the whole railway system with the outside world
EN 50121-3	Railway applications - Electromagnetic compatibility (EMC) - Rolling stock
EN 50121-4	Railway applications - Electromagnetic compatibility (EMC) - Signalling and communications
EN 50124-1	Railway applications - Insulation co-ordination - Basic requirements, clearances and creepage distances
EN 50124-3	Railway applications - Insulation co-ordination - Solid and liquid insulations
EN 50125-1	Railway applications - Environmental conditions for equipment - Equipment on board rolling stock
EN 50125-3	Railway applications - Environmental conditions for equipment - Signalling and communications
EN 50126	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
EN 50128	Railway applications - Software for railway control and protection systems
EN 50155	Railway applications - Electronic equipment used on rail vehicles
EN 50159-1	Railway applications - Signalling and communications - Safety-related communication in closed transmission systems
EN 50159-2	Railway applications - Signalling and communications - Safety-related communication in open transmission 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 assessor: The person or agent appointed to carry out the assessment.

3.1.4 authorisation: The formal permission to use a product within specified application constraints.

3.1.5 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.

3.1.6 can Is possible.

3.1.7 common-mode fault: Fault common to items which are intended to be independent.

3.1.8 component: See **element**

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 pre-build exercise of defining elements and their interconnection such that the product will meet its specified requirements.

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 **designer**: One or more persons assigned by the Design Authority to analyse and transform specified requirements into acceptable design solutions which have the required safety integrity.

3.1.14 **diversity:** A means of achieving all or part of the specified requirements in more than one independent and dissimilar manner.

3.1.15 **element:** A part of a product that has been determined to be a basic unit or building block. An element may be simple or complex.

3.1.16 **equipment**: A functional physical item.

3.1.17 **error**: A deviation from the intended design which could result in unintended system behaviour or failure.

3.1.18 **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.

3.1.19 **failure**: A deviation from the specified performance of a system. A failure is the consequence of an fault or error in the system.

3.1.20 **fault**: An abnormal condition that could lead to an error in a system. A fault can be random or systematic.

3.1.21 **fault detection time**: Time span which begins at the instant when a fault occurs and ends when the existence of the fault is detected.

3.1.22 **hazard**: A condition that could lead to an accident.

3.1.23 **hazard analysis:** The process of identifying the hazards which a product or its use can cause.

3.1.24 **hazard log:** The document in which all safety management activities, hazards identified, decisions made and solutions adopted, are recorded or referenced.

3.1.25 human error: A human action (mistake), which can result in unintended system behaviour/failure.

3.1.26 independence (human): Freedom from intellectual, commercial and/or management involvement.

3.1.27 independence (technical): Freedom from any mechanism which can affect the correct operation of more than one item.

3.1.28 item: Element under consideration.

3.1.29 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.

3.1.30 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.

3.1.31 may: Is permissible.

3.1.32 negation: Enforcement of a safe state following detection of a hazardous fault.

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

3.1.34 product: A collection of elements, interconnected to form a system, subsystem or item of equipment, in a manner which meets the specified requirements.

3.1.35 quality: A user perception of the attributes of a product.

3.1.36 railway authority: The body with the overall accountability to a safety authority for operating a safe railway system

3.1.37 random failure integrity: The degree to which a system is free from hazardous random faults.

3.1.38 random fault: The occurrence of a fault based on probability theory and previous performance.

3.1.39 redundancy: The provision of one or more additional elements, usually identical, to achieve or maintain availability under the failure of one or more of those elements.

3.1.40 reliability: The ability of an item to perform a required function under given conditions for a given period of time.

3.1.41 repair: Measures for re-establishing the required state of a system, subsystem or item of equipment.

3.1.42 risk: The combination of the frequency, or probability, and the consequence of a specified hazardous event.

3.1.43 safe state: A condition which continues to preserve safety.

3.1.44 safety. Freedom from unacceptable levels of risk.

3.1.45 safety acceptance: The safety status given to a product by the final user.

3.1.46 safety acceptance process: The series of procedures that are followed to achieve safety acceptance

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 Approval process: The series of procedures that are followed to achieve Safety Approval.

3.1.49 safety assessment: The process of analysis to determine whether the design authority and the validator have achieved a product that meets the specified safety requirements and to form a judgement as to whether the product is safe for its intended purpose.

3.1.50 safety assessor: The person or agent appointed to carry out the safety assessment.