Raudteealased rakendused. Side-, signalisatsiooni- ja andmetöötlussüsteemid. Ohutusalane andmeside

Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-EN 50159:2010 sisaldab Euroopa standardi EN 50159:2010 ingliskeelset teksti.	This Estonian standard EVS-EN 50159:2010 consists of the English text of the European standard EN 50159:2010.
Standard on kinnitatud Eesti Standardikeskuse 31.10.2010 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.	This standard is ratified with the order of Estonian Centre for Standardisation dated 31.10.2010 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.
Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 17.09.2010.	Date of Availability of the European standard text 17.09.2010.
Standard on kättesaadav Eesti standardiorganisatsioonist.	The standard is available from Estonian standardisation organisation.

ICS 35.240.60, 45.020

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50159

September 2010

ICS 35.240.60; 45.020

Supersedes EN 50159-1:2001, EN 50159-2:2001

English version

Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante Kommunikation in Übertragungssystemen

This European Standard was approved by CENELEC on 2010-09-01. 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, 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, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 50159:2010 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. It was submitted to the formal vote and was approved by CENELEC as EN 50159 on 2010-09-01.

This document supersedes EN 50159-1:2001 and EN 50159-2:2001.

The contents of both standards have been merged; the informative Annex E gives a mapping between these previous editions and the present document.

This European Standard is closely related to EN 50129:2003.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

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)	2011-09-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2013-09-01

This draft European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and covers essential requirements of EC Directives 96/48/EC (HSR), recast by EC Directives 2008/57/EC (RAIL). See Annex ZZ.

Contents

Figures

Tables

Introduction

If a safety-related electronic system involves the transfer of information between different locations, the transmission system then forms an integral part of the safety-related system and it shall be shown that the end to end communication is safe in accordance with EN 50129.

The transmission system considered in this standard, which serves the transfer of information between different locations, has in general no particular preconditions to satisfy. It is from the safety point of view not trusted, or not fully trusted.

The standard is dedicated to the requirements to be taken into account for the communication of safety-related information over such transmission systems.

Although the RAM aspects are not considered in this standard it is recommended to keep in mind that they are a major aspect of the global safety.

The safety requirements depend on the characteristics of the transmission system. In order to reduce the complexity of the approach to demonstrate the safety of the system, transmission systems have been classified into three categories:

– Category 1 consists of systems which are under the control of the designer and fixed during their lifetime;

– Category 2 consists of systems which are partly unknown or not fixed, however unauthorised access can be excluded;

– Category 3 consists of systems which are not under the control of the designer, and where unauthorised access has to be considered.

The first category was covered by EN 50159-1:2001, the others by EN 50159-2:2001.

When safety-related communication systems, which have been approved according to the previous standards, are subject of maintenance and/or extensions, the informative Annex E can be used for traceability purposes of (sub)clauses of this standard with the (sub)clauses of the former series.

1 Scope

This European Standard is applicable to safety-related electronic systems using for digital communication purposes a transmission system which was not necessarily designed for safety-related applications and which is

– under the control of the designer and fixed during the lifetime, or

– partly unknown or not fixed, however unauthorised access can be excluded, or

– not under the control of the designer, and also unauthorised access has to be considered.

Both safety-related equipment and non safety-related equipment can be connected to the transmission system.

This standard gives the basic requirements needed to achieve safety-related communication between safety-related equipment connected to the transmission system.

This European Standard is applicable to the safety requirement specification of the safety-related equipment connected to the transmission system, in order to obtain the allocated safety integrity requirements.

Safety requirements are generally implemented in the safety-related equipment, designed according to EN 50129. In certain cases these requirements may be implemented in other equipment of the transmission system, as long as there is control by safety measures to meet the allocated safety integrity requirements.

The safety requirement specification is a precondition of the safety case of a safety-related electronic system for which the required evidence is defined in EN 50129. Evidence of safety management and quality management has to be taken from EN 50129. The communication-related requirements for evidence of functional and technical safety are the subject of this standard.

This European Standard is not applicable to existing systems, which had already been accepted prior to the release of this standard.

This European Standard does not specify

– the transmission system,

– equipment connected to the transmission system,

– solutions (e.g. for interoperability),

– which kind of data are safety-related and which are not.

A safety-related equipment connected through an open transmission system can be subjected to many different IT security threats, against which an overall program has to be defined, encompassing management, technical and operational aspects.

In this European Standard however, as far as IT security is concerned, only intentional attacks by means of messages to safety-related applications are considered.

This European Standard does not cover general IT security issues and in particular it does not cover IT security issues concerning

– ensuring confidentiality of safety-related information,

– preventing overloading of the transmission system.

2 Normative references

The following referenced documents are indispensable for the application 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.

CLC/TR / EN 50126 series, *Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*

EN 50129:2003, *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

3.1.1
absolute time stamp
time stamp referenced to a global time which is common for a group of entities using a transmission system

3.1.2
access protection
processes designed to prevent unauthorised access to read or to alter information, either within user safety-related systems or within the transmission system

3.1.3
additional data
data which is not of any use to the ultimate user processes, but is used for control, availability, and safety purposes

3.1.4
authentic message
message in which information is known to have originated from the stated source

3.1.5
authenticity
state in which information is valid and known to have originated from the stated source

3.1.6
closed transmission system
fixed number or fixed maximum number of participants linked by a transmission system with well known and fixed properties, and where the risk of unauthorised access is considered negligible

3.1.7
communication
transfer of information between applications

3.1.8
confidentiality
property that information is not made available to unauthorised entities

3.1.9
corrupted message
type of message error in which a data corruption occurs