

© Copyright SEK. Reproduction in any form without permission is prohibited.

Järnvägsanläggningar – System för telekommunikation, signal- och processtyrning – Överföring av säkerhetsrelaterade data i teletransmissionssystem

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

Som svensk standard gäller europastandarden EN 50159:2010. Den svenska standarden innehåller den officiella engelska språkversionen av EN 50159:2010.

Nationellt förord

Tidigare fastställd svensk standard SS-EN 50159-1, utgåva 1, 2001, SS-EN 50159-1 C1, utgåva 1, 2010, SS-EN 50159-2, utgåva 1, 2001 och SS-EN 50159-2 C1, utgåva 1, 2010, gäller ej fr o m 2013-09-01.

ICS 35.240.60; 45.020

Denna standard är fastställd av SEK Svensk Elstandard, som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: SEK, Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00. Telefax: 08 - 444 14 30
E-post: sek@elstandard.se. Internet: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

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

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

Introduction	5
1 Scope	6
2 Normative references	7
3 Terms, definitions and abbreviations	7
3.1 Terms and definitions	7
3.2 Abbreviations	12
4 Reference architecture	13
5 Threats to the transmission system	16
6 Classification of transmission systems	17
6.1 General	17
6.2 General aspects of classification	17
6.3 Criteria for the classification of transmission systems	17
6.4 Relationship between transmission systems and the threats	18
7 Requirements for defences	18
7.1 Preface	18
7.2 General requirements	19
7.3 Specific defences	20
7.4 Applicability of defences	26
Annex A (informative) Threats on open transmission systems	28
A.1 System view	28
A.2 Derivation of the basic message errors	29
A.3 Threats	30
A.4 A possible approach for building a safety case	31
A.5 Conclusions	35
Annex B (informative) Categories of transmission systems	37
B.1 Categories of transmission systems	37
B.2 Relationship between the category of transmission systems and threats	39
Annex C (informative) Guideline for defences	40
C.1 Applications of time stamps	40
C.2 Choice and use of safety codes and cryptographic techniques	41
C.3 Safety code	46
C.4 Length of safety code	49
C.5 Communication between safety-related and non safety-related applications	51
Annex D (informative) Guidelines for use of the standard	53
D.1 Procedure	53
D.2 Example	54
Annex E (informative) Mapping from previous standards	59
Annex ZZ (informative) Coverage of Essential Requirements of EC Directives	62
Bibliography	63

Figures

Figure 1 – Reference architecture for safety-related communication.....	15
Figure 2 – Cyclic transmission of messages	21
Figure 3 – Bi-directional transmission of messages	22
Figure A.1 – Hazard tree	29
Figure A.2 – Causes of threats	32
Figure C.1 – Classification of the safety-related communication system	42
Figure C.2 – Model of message representation within the transmission system (Type A0, A1)	43
Figure C.3 – Use of a separate access protection layer.....	44
Figure C.4 – Model of message representation within the transmission system (Type B0).....	45
Figure C.5 – Model of message representation within the transmission system (Type B1).....	46
Figure C.6 – Basic error model.....	49
Figure C.7 – Communication between non safety-related and safety-related applications.....	52
Figure D.1 – Fault tree for the hazard “accident”	55
Figure D.2 – Fault tree for case 1	56
Figure D.3 – Fault tree for case 2.....	58

Tables

Table 1 – Threats/Defences matrix	26
Table A.1 – Relationship between hazardous events and threats.....	36
Table B.1 – Categories of transmission systems	38
Table B.2 – Threat/Category relationship	39
Table C.1 – Assessment of the safety encoding mechanisms	48
Table E.1 – Mapping from EN 50159-1:2001 into EN 50159:201X.....	60
Table E.2 – Mapping from EN 50159-2:2001 into EN 50159:201X.....	61

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*