SLOVENSKI STANDARD
SIST EN 50159:2010

01-november-2010

Nadomešča:
SIST EN 50159-1:2002
SIST EN 50159-2:2002

Železniške naprave - Komunikacijski, signalni in procesni sistemi - Varnostna komunikacija v prenosnih sistemih

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc83-4d90-8a74-55b15e901a09/sist-en-50159-2010

Ta slovenski standard je istoveten z: **EN 50159:2010**

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 50159:2010 **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST EN 50159:2010

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc83-4d90-8a74-55b15e901a09/sist-en-50159-2010

SIST EN 50159:2010

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc83-4d90-8a74-55b15e901a09/sist-en-50159-2010

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

© 2010 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

SIST EN 50159:2010

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc83-4d90-8a74-55b15e901a09/sist-en-50159-2010

SIST EN 50159:2010

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc83-4d90-8a74-56b15e901a09/sist-en-50159-2010

SIST EN 50159:2010

Figures

Tables

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc83-4d90-8a74-55015c901a09/sist-en-50159-2010

SIST EN 50159:2010

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-ce83-4d00-8a74-55b15c901a09/sist-en-50159-2010

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.

SIST EN 50159:2010

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc83-4d90-8a74-55b15c901e09/sist-en-50159-2010

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.

SIST EN 50159:2010

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc83-4d90-8a74-55b15e901a09/sist-en-50159-2010

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

SIST EN 50159:2010

3.1.10
cryptographic techniques
producing output data, calculated by an algorithm using input data and a key as a parameter

NOTE By knowing the output data, it is impossible within a reasonable time to calculate the input data without knowledge of the key. It is also impossible within a reasonable time to derive the key from the output data, even if the input data are known.

3.1.11
cyclic redundancy check
cyclic code, used to protect messages from the influence of data corruption

3.1.12
data
part of a message which represents some information (see also user data, additional data, redundant data)

3.1.13
data corruption
alteration of data

3.1.14
defence
measure incorporated in the design of a safety-related communication system to counter particular threats

3.1.15
delayed message
type of message error in which a message is received at a time later than intended

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.16
deleted message
type of message error in which a message is removed from the message stream

SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc83-4d90-8a74-55b15e901a09/sist-en-50159-2010

3.1.17
double time stamp
case when two entities exchange and compare their time stamps. In this case the time stamps in the entities are independent of each other

3.1.18
error
deviation from the intended design which could result in unintended system behaviour or failure

3.1.19
failure
deviation from the specified performance of a system

NOTE A failure is the consequence of a fault or an error in the system.

3.1.20
fault
abnormal condition that could lead to an error in a system

NOTE A fault can be random or systematic.

3.1.21
feedback message
response from a receiver to the sender, via a return channel

3.1.22
hacker
person trying deliberately to bypass access protection

SIST EN 50159:2010

3.1.23
hazard
condition that can lead to an accident

3.1.24
hazard analysis
process of identifying hazards and analysing their causes, and the derivation of requirements to limit the likelihood and consequences of hazards to an acceptable level

3.1.25
implicit data
additional data that is not transmitted but is known to the sender and receiver

3.1.26
information
representation of the state or events of a process, in a form understood by the process

3.1.27
inserted message
type of message error in which an additional message is implanted in the message stream

3.1.28
integrity
state in which information is complete and not altered

3.1.29
manipulation detection code
function of the whole message without secret key

NOTE In contrast to a MAC there is no secret key involved. By the whole message is meant also any implicit data of the message which is not sent to the transmission system. The MDC is often based on a hash function.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc83-4d90-8a74-55b15e901a09/sist-en-50159-2010

3.1.30
masqueraded message
type of inserted message in which a non-authentic message is designed to appear to be authentic

3.1.31
message
information which is transmitted from a sender (data source) to one or more receivers (data sink)

3.1.32
message authentication code
cryptographic function of the whole message and a secret or public key

NOTE By the whole message is meant also any implicit data of the message which is not sent to the transmission system.

3.1.33
message enciphering
transformation of bits by using a cryptographic technique within a message, in accordance with an algorithm controlled by keys, to render casual reading of data more difficult. Does not provide protection against data corruption

3.1.34
message errors
set of all possible message failure modes which can lead to potentially dangerous situations, or to reduction in system availability. There can be a number of causes of each type of error

3.1.35
message integrity
message in which information is complete and not altered

SIST EN 50159:2010

3.1.36
message stream
ordered set of messages

3.1.37
non cryptographic safety code
redundant data based on non-cryptographic functions included in a safety-related message to permit data corruption to be detected by the safety-related transmission function

3.1.38
open transmission system
transmission system with an unknown number of participants, having unknown, variable and non-trusted properties, used for unknown telecommunication services and having the potential for unauthorised access

3.1.39
random failure
failure that occurs randomly in time

3.1.40
redundancy check
type of check that a predefined relationship exists between redundant data and user data within a message, to prove message integrity

3.1.41
redundant data
additional data, derived, by a safety-related transmission function, from the user data

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.42
relative time stamp
time stamp referenced to the local clock of an entity. In general there is no relationship to clocks of other entities

SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc83-4d90-8a74-55b15e901a09/sist-en-50159-2010

3.1.43
repeated message
type of message error in which a single message is received more than once

3.1.44
re-sequenced message
type of message error in which the order of messages in the message stream is changed

3.1.45
safe fall back state
safe state of a safety-related equipment or system as a deviation from the fault-free state and as a result of a safety reaction leading to a reduced functionality of safety-related functions, possibly also of non safety-related functions

3.1.46
safety
freedom from unacceptable levels of risk

3.1.47
safety case
documented demonstration that the product complies with the specified safety requirements

3.1.48
safety code
redundant data included in a safety-related message to permit data corruptions to be detected by the safety-related transmission function

SIST EN 50159:2010

3.1.49
safety integrity level
number which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures

3.1.50
safety reaction
safety-related protection taken by the safety process in response to an event (such as a failure of the transmission system), which may lead to a safe fall back state of the equipment

3.1.51
safety-related
carries responsibility for safety

3.1.52
safety-related transmission function
function incorporated in the safety-related equipment to ensure authenticity, integrity, timeliness and sequence of data

3.1.53
sequence number
additional data field containing a number that changes in a predefined way from message to message

3.1.54
source and destination identifier
identifier which is assigned to each entity. This identifier can be a name, number or arbitrary bit pattern. This identifier will be used for the safety-related communication. Usually the identifier is added to the user data

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/e02dc220-cc83-4d90-8a74-
55b15e901a09/sist-en-50159-2010

3.1.55
systematic failure
failure that occurs repeatedly under some particular combination of inputs, or under some particular environmental condition

3.1.56
threat
potential violation of safety

3.1.57
time stamp
information concerning time of transmission attached to a message by the sender

3.1.58
timeliness
state in which information is available at the right time according to requirements

3.1.59
transmission code
redundant information, added to the safety and non safety message of the non-trusted transmission system in order to ensure the integrity of the message during transmission

3.1.60
transmission system
service used by the application to communicate message streams between a number of participants, who may be sources or sinks of information

3.1.61
trusted
which has properties used as evidence to support the safety demonstration

SIST EN 50159:2010

3.1.62
unauthorised access
situation in which user information or information within the transmission system is accessed and/or changed by unauthorised persons or hackers

3.1.63
user data
data which represents the states or events of a user process, without any additional data. In case of communication between safety-related equipment, the user data contains safety-related data

3.1.64
valid message
message whose form meets in all respects the specified user requirements

3.1.65
validity
state of meeting in all respects the specified user requirements

3.2 Abbreviations

For the purpose of this document, the following abbreviations apply.

BCH	Bose, Ray-Chaudhuri, Hocquenghem Code
B.M.E.	Basic Message Errors
BSC	Binary Symmetric Channel
CAN	Controller Area Network
CRC	Cyclic Redundancy Check
EC	European Community
ECB	Electronic CodeBook mode
EMI	Electromagnetic Interference
FTA	Fault Tree Analysis
GPRS	General Packet Radio Service
GSM-R	Global System for Mobile communication – Railways
H.E.	Hazardous Events
HW	Hardware
IT	Information Technology
LAN	Local Area Network
MAC	Message Authentification Code
MDC	Manipulation Detection code
MD4, MD5	Message Digest algorithms
M.H.	Main Hazard
MTBF	Mean Time Between Failures
MVB	Multi-purpose Vehicle Bus
PROFIBUS	Process Field Bus
QSC	q-nary symmetric channel
RAMS	Reliability, Availability, Maintainability and Safety
SIL	Safety Integrity Level
SR	Safety Related

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc83-4d90-8a74-55b15c901a09/sist-en-50159-2010

SIST EN 50159:2010

SRS	Safety Requirements Specifications
SW	Software
TX	Transmission
UTC	Universal Coordinated Time
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity

4 Reference architecture

This European Standard defines the safety requirements for the safe communication between safety-related equipment via a transmission system, which can either be closed or open. Both, safety-related and non safety-related equipment can be connected to the transmission system. This clause describes possible configurations of the safety-related communication in transmission systems including the definition of involved functional blocks. Particular requirements to be fulfilled by these blocks are specified in further clauses.

A combined view – open and closed transmission system – of the principal architecture is shown in Figure 1, where all communication elements are linked according to the information flow to exchange safety-related information between safety-related equipment. The reference architecture also shows a non-safety-related interface which is not always present. A typical use could be for diagnostic messages routed to a maintenance centre.

Besides the source and destination of safety-related communication the reference architecture deals with a safety-related communication system, which can be divided into

- safety-related transmission functions incorporated in the safety-related equipment. These functions ensure authenticity, integrity, timeliness and sequence of data,
- safety-related cryptographic techniques which protect the safety-related message. These can either be realised by incorporating them in the safety-related equipment or having them outside of the safety-related equipment but checked by safety techniques. These techniques protect the safety-related message in a Category 3 transmission system and are not needed in the case of a Category 1 or 2 transmission system,
- a non safety-related, open or closed transmission system which may itself include transmission protection functions and/or access protection functions.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50159:2010
https://standards.iteh.ai/catalog/standards/sist/c02dc220-cc33-4d90-8a74-55b15e901a09/sist-en-50159-2010

The characteristics of closed transmission systems (Category 1) are as follows:

- the number of pieces of connectable equipment – either safety-related or not – to the transmission system is known and fixed;
- the risk of unauthorized access is considered negligible;
- the physical characteristics of the transmission system (e.g. transmission media, environment according to design hypothesis, etc.) are fixed and unchanged during the life cycle of the system.

The open transmission system (Category 2 and/or 3) can contain some or all of the following:

- elements which read, store, process or re-transmit data produced and presented by users of the transmission system in accordance with a program not known to the user. The number of users is generally unknown, and safety-related and non safety-related equipment, and equipment which is not related to railway applications, can be connected to the open transmission system;
- transmission media of any type with transmission characteristics and susceptibility to external influences, which are unknown to the user;