SLOVENSKI STANDARD
SIST EN 50159:2026

01-oktober-2026

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

Ta slovenski standard je istoveten z: **EN 50159:2026**

ICS:

35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport
45.020	Železniška tehnika na splošno	Railway engineering in general

SIST EN 50159:2026 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50159

July 2026

ICS 35.240.60; 45.020

Supersedes EN 50159:2010; EN 50159:2010/A1:2020

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 2026-06-15. 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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre 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, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. EN 50159:2026 E

Contents

Page

European foreword

This document (EN 50159:2026) has been prepared by CLC/SC 9XA “Communication, signalling and processing systems”.

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2027-07-31
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2029-07-31

This document supersedes EN 50159:2010 and all of its amendments and corrigenda.

EN 50159:2026 includes the following significant technical changes with respect to EN 50159:2010:

Requirements and guidance have been added on the following topics:

— Clause 3: harmonization of terminology, in particular with cybersecurity domain;

— Clauses 4 and 7.2: generalization to cover mixed safety integrity contexts;

— Clauses 6 and 7.2: coordination of cybersecurity requirements for Category 3 transmission systems;

— Clause C.6: guidance on separation between safety and cybersecurity;

— Annex D: guidance on the change management process for railway duty holders.

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

Any feedback and questions on this document should be directed to the users’ national committee. A complete listing of these bodies can be found on the CENELEC website.

Introduction

If a safety-related electronic system involves communication of information, the transmission system forms an integral part of the safety-related system and it is understood that the communication is safe in accordance with EN 50129, with respect to random and systematic faults.

The transmission system considered in this document, 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.

This document 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 document, it is recommended to keep in mind that they are a major aspect of the operational 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: closed transmission systems;

— Category 2 and Category 3: open transmission systems.

For safety purposes application messages using Category 3 transmission systems need protection against unauthorized access that can corrupt the integrity of data. This document only provides general requirements to protect in case of Category 3 transmission systems. For a complete set of cybersecurity requirements, specific cybersecurity standards are applicable.

1 Scope

This document is applicable to safety-related electronic systems using for digital communication purposes a transmission system which was not necessarily designed for safety-related applications. For transmission systems where the risk of unauthorized access is not negligible, the document defines the interface to the applicable cybersecurity standards.

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

This document gives the specific requirements needed to achieve safety-related communication between safety-related equipment connected to the transmission system, while the general system requirements including allocation of safety requirements and content of the safety case are defined in EN 50129.

This document is not applicable to existing systems which had already been accepted prior to the release of this document. However, so far as reasonably practicable, it is applicable to modifications and extensions to existing systems, subsystems and equipment.

This document 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 cybersecurity threats, against which an overall program is defined encompassing management, technical and operational aspects.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

EN 50129, *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*

CLC/TS 50701:2023, *Railway applications - Cybersecurity*

EN IEC 63452,[1] *Railway applications – Cybersecurity (IEC 63452)*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org

[1] Under preparation. Stage at the time of publication: prEN IEC 63452:2025.

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

[SOURCE: IEC 60050-821:2017, 821-11-01]

3.1.2
access control
protection of system resources against unauthorized access

Note 1 to entry: Unauthorized access can be physical or logical. In this document, this definition applies only to logical access to data transmission.

[SOURCE: CLC/TS 50701:2023, 3.1.3, modified — Note 1 to entry has been added.]

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

[SOURCE: IEC 60050-821:2017, 821-11-03]

3.1.4
attack
attempt to gain access to an information processing system in order to produce damage

Note 1 to entry: The damage can be e.g. destruction, disclosure, alteration, disruption, unauthorized use.

Note 2 to entry: In this document, this definition applies only to data transmission.

[SOURCE: CLC/TS 50701:2023, 3.1.12, modified — Note 2 to entry has been added.]

3.1.5
authentic message
message in which information is known to have originated from the stated source

[SOURCE: IEC 50050-821:2017, 821-11-04]

3.1.6
authenticity
state in which information is known to have originated from the stated source

[SOURCE: IEC 60050-821:2017, 821-11-05, modified — “valid and” has been removed.]

3.1.7
basic message error
message error such as repetition, deletion, insertion, re-sequencing, corruption, delay and masquerade

3.1.8
closed transmission system
transmission system with a fixed number or fixed maximum number of participants having well-known and fixed properties, and where the risk of unauthorized access is negligible

[SOURCE: IEC 60050-821:2017, 821-11-06, modified – “transmission system with a” has been added. “linked by a transmission system with” has been replaced with “having”. “considered” has been removed.]

3.1.9
communication
information transfer according to agreed conventions

[SOURCE: IEC 60050-701:2016, 701-01-04]

3.1.10
conduit
<cybersecurity> logical grouping of communication channels, connecting two or more zones, that share common security requirements

Note 1 to entry: A conduit is allowed to traverse a zone as long as the security of the channels contained within the conduit is not impacted by the zone.

[SOURCE: EN IEC 62443-4-2:2019, 3.1.11]

3.1.11
confidentiality
<cybersecurity> assurance that information is not disclosed to unauthorized individuals, processes, or devices

[SOURCE: CLC/TS 50701:2023, 3.1.27]

3.1.12
corrupted message
type of message error in which a data corruption occurs

[SOURCE: IEC 60050-821:2017, 821-11-08]

3.1.13
countermeasure
<cybersecurity> action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

[SOURCE: CLC/TS 50701:2023, 3.1.1, modified – Note 1 to entry has been omitted.]

3.1.14
cryptographic algorithm
algorithm based on the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.3, modified - “upon” has been replaced with “on”.]

3.1.15
cryptographic safety code
safety code based on a cryptographic algorithm

Note 1 to entry: A cryptographic safety code can be based on a cryptographic algorithm, which exhibits weaknesses with regards to security. In the safety context only the properties for error detection of the cryptographic safety code are relevant (rather than resistance to intentional attacks).

3.1.16
cybersecurity
<railway application> set of activities and measures taken with the objective to identify, protect against, detect, respond to, and recover from unauthorized access or cyberattack which could lead to an accident, an unsafe situation, or railway application performance degradation

Note 1 to entry: It is recognized that the term “cybersecurity” has a broader meaning in other standards and guidance, often including non-malevolent threats, human errors, and protection against natural disasters. Those aspects, except human errors degrading security controls, are not included in this document.

[SOURCE: CLC/TS 50701:2023, 3.1.32]

3.1.17
cyclic redundancy check
<communication in transmission systems> cyclic code used to protect messages from the influence of data corruption

[SOURCE: IEC 60050-821:2017, 821-11-10]

3.1.18
data
<communication in transmission systems> part of a message which represents some information

Note 1 to entry: See also user data, additional data, redundant data.

[SOURCE: IEC 60050-821:2017, 821-11-11, modified – Note 1 to entry has been added.]

3.1.19
data corruption
alteration of data

[SOURCE: IEC 60050-821:2017, 821-11-13]

3.1.20
defence
measure incorporated in the design of a safety-related communication system to counter particular hazards

[SOURCE: IEC 60050-821:2017, 821-11-14, modified – “safety” has been replaced with “safety-related”. “threats” has been replaced with “hazards”.]

3.1.21
delayed message
type of message error in which a message is received at a time later than intended

[SOURCE: IEC 60050-821:2017, 821-11-15]

3.1.22
deleted message
type of message error in which a message is removed from the message stream

[SOURCE: IEC 60050-821:2017, 821-11-16]

3.1.23
double time stamp
case when two entities exchange and compare their time stamps

Note 1 to entry: In this case the time stamps in the entities are independent of each other.

[SOURCE: IEC 60050-821:2017, 821-11-17]

3.1.24
encryption
<data> transformation of data in order to hide their semantic content using cryptography

Note 1 to entry: The reverse process is called decryption.

Note 2 to entry: In former version of this document the term “enciphering” was used.

[SOURCE: IEC 60050-171:2019, 171-08-09, modified — Note 2 to entry has been added.]

3.1.25
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

Note 1 to entry: An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.

Note 2 to entry: A human error can be seen as a human action or inaction that can produce an unintended result.

[SOURCE: IEC 60050-192:2024, 192-03-02, modified – Notes 1 and 2 to entry have been modified.]

3.1.26
failure
<item> loss of ability to perform as required

Note 1 to entry: Qualifiers, such as catastrophic, critical, major, minor, marginal and insignificant, can be used to categorize failures according to the severity of consequences, the choice and definitions of severity criteria depending upon the field of application.

Note 2 to entry: Qualifiers, such as misuse, mishandling and weakness, can be used to categorize failures according to the cause of failure.

Note 3 to entry: “Failure” is an event, as distinguished from “fault”, which is a state.

[SOURCE: IEC 60050-821:2017, 821-11-19, modified – “may” has been changed with “can” in notes 1 and 2 to entry. Note 3 to entry has been added.]

3.1.27
fault
<system> abnormal condition that could lead to an error in a system

Note 1 to entry: A fault can be random or systematic.

[SOURCE: IEC 60050-821:2017, 821-11-20]

3.1.28
feedback message
response from a receiver to the sender, via a return channel

[SOURCE: IEC 60050-821:2017, 821-11-21]

3.1.29
hazard
<railway> condition that can lead to an accident

[SOURCE: EN 50129:2018, 3.1.21, modified – Note 1 to entry has been omitted.]

3.1.30
hazard analysis
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

[SOURCE: IEC 60050-821:2017, 821-11-23]

3.1.31
hazardous event
event that can cause harm

Note 1 to entry: A hazardous event can occur over a short period of time or over an extended period of time.

[SOURCE: IEC 60050-903:2013, 903-01-04]

3.1.32
implicit data
additional data that is not transmitted but is known to the sender and receiver

[SOURCE: IEC 60050-821:2017, 821-11-12]

3.1.33
information
knowledge concerning objects, such as facts, events, things, processes, or ideas (including concepts) that, within a certain context, has a particular meaning

Note 1 to entry: Information can be represented for example by signs, symbols, pictures or sounds.

[SOURCE: IEC 60050-171:2019, 171-01-01]

3.1.34
inserted message
type of message error in which an additional message is implanted in the message stream

[SOURCE: IEC 60050-821:2017, 821-11-25, modified – “type of message error in which an” and “is” have been added. “which leads to an error” has been removed.]

3.1.35
integrity
<information>state in which information is complete and not altered

[SOURCE: IEC 60050-821:2017, 821-11-26]

3.1.36
manipulation detection code
function of the whole message without a secret key

Note 1 to entry: 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 are not sent to the transmission system. The MDC is often based on a hash function.

[SOURCE: IEC 60050-821:2017, 821-11-27, modified – Some editorial corrections in the note 1 to entry.]

3.1.37
masqueraded message
type of inserted message in which a non-authentic message is intentionally designed to appear to be authentic

[SOURCE: IEC 60050-821:2017, 821-11-28, modified – “non-authentic” has been replaced with “type of”. “which is” has been replaced with “in which a non-authentic message is intentionally”.]

3.1.38
message
<transmission systems> information which is transmitted in one or several packets from a sender to one or more receivers

[SOURCE: IEC 60050-821:2017, 821-11-29]

3.1.39
message authentication code
cryptographic function of the whole message and a secret or public key

Note 1 to entry: By the whole message is meant also any implicit data of the message which is not sent to the transmission system.

[SOURCE: IEC 60050-821:2017, 821-11-30, modified – Some editorial corrections in the note 1 to entry.]

3.1.40
message errors
set of all possible message failure modes which can lead to potentially dangerous situations, or to reduction in system availability

Note 1 to entry: There can be a number of causes of each type of error.

[SOURCE: IEC 60050-821:2017, 821-11-32]

3.1.41
message integrity
message in which information is complete and not altered

[SOURCE: IEC 60050-821:2017, 821-11-33]

3.1.42
message stream
ordered set of messages

[SOURCE: IEC 60050-821:2017, 821-11-34]

3.1.43
negligible risk
risk which is so low that it is not reasonable to implement additional measures

Note 1 to entry: The risk of unauthorized access to the transmission system can be treated as negligible if the location and physical security of all points at which an item of equipment could be connected to the transmission system is such that it is not credible that a potential attacker could gain access.

Note 2 to entry: Negligible risks are considered as insignificant and adequately controlled without defining further requirements.

3.1.44
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 unauthorized access

Note 1 to entry: In this document an open transmission system designates a transmission system of Category 2 or Category 3.

[SOURCE: IEC 60050-821:2017, 821-11-36, modified – Note 1 to entry has been added.]

3.1.45
railway duty holder
body with the overall accountability for operating a railway system within the legal framework

Note 1 to entry: Railway duty holder accountabilities for the overall system or its parts and life cycle activities are sometimes split between one or more bodies or entities. For example:

— the owner(s) of one or more parts of the system assets and their purchasing agents;

— the operator of the system;

— the maintainer(s) of one or more parts of the system.

Note 2 to entry: Typically, the railway duty holders are railway undertakings and the infrastructure managers. Such splits are based on either statutory instruments or contractual agreements. Such responsibilities are defined at the earliest stages of a system life cycle.

[SOURCE: EN 50126-1:2017, 3.48]

3.1.46
random failure
failure that occurs randomly in time

[SOURCE: IEC 60050-821:2017, 821-11-38]

3.1.47
redundancy check
type of check that a predefined relationship exists between redundant data and user data within a message, to prove message integrity

[SOURCE: IEC 60050-821:2017, 821-11-39]

3.1.48
redundant data
additional data, derived from the user data, by a safety-related transmission function

[SOURCE: IEC 60050-821:2017, 821-11-40]

3.1.49
relative time stamp
time stamp referenced to the local clock of an entity

Note 1 to entry: In general, there is no relationship to clocks of other entities.

[SOURCE: IEC 60050-821:2017, 821-11-41]

3.1.50
repeated message
type of message error in which a single message is received more than once

[SOURCE: IEC 60050-821:2017, 821-11-42]

3.1.51
re-sequenced message
type of message error in which the order of messages in the message stream is changed

[SOURCE: IEC 60050-821:2017, 821-11-43]

3.1.52
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

[SOURCE: IEC 60050-821:2017, 821-11-44, modified – “and possibly” has been replaced with “possibly”. “non-safety-related” has been replaced with “non-safety-related”.]

3.1.53
safety
freedom from unacceptable risk

[SOURCE: IEC 60050-903:2013, 903-01-19]

3.1.54
safety case
documented demonstration that the product (e.g. a system, subsystem or equipment) complies with the specified safety requirements

[SOURCE: IEC 60050-821:2017, 821-12-53]

3.1.55
safety code
redundant data included in a safety-related message to permit data corruptions to be detected by the safety-related transmission function

Note 1 to entry: Also, codes based on cryptographic algorithms can be used as safety codes such as hash block codes or MAC with fixed keys. For such cryptographic safety codes the same requirements apply.

[SOURCE: IEC 60050-821:2017, 821-11-45, modified – Note 1 to entry has been added.]

3.1.56
safety integrity level
one of a number of defined discrete levels for specifying the safety integrity requirements of safety-related functions allocated to the safety-related systems

3.1.57
safety reaction
safety-related protection taken by the safety process in response to an event (such as a failure of the transmission system), which can lead to a safe fall back state of the equipment

[SOURCE: IEC 60050-821:2017, 821-11-47]

3.1.58
safety-related
carries responsibility for safety

Note 1 to entry: A function, component, product, system, or procedure is called safety-related if at least one of its properties is used in the safety argument for the system in which it is applied. These properties can be of functional or non-functional nature.

[SOURCE: IEC 60050-821:2017, 821-01-73, modified – Note 1 to entry has been added.]

3.1.59
safety-related transmission function
function incorporated in the safety-related equipment to ensure authenticity, integrity, timeliness and sequence of data