SLOVENSKI STANDARD
oSIST prEN 50159:2025

01-marec-2025

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: **prEN 50159**

ICS:

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

oSIST prEN 50159:2025 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 50159

January 2025

ICS 35.240.60; 45.020

Will supersede 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 draft European Standard is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2025-04-11.

It has been drawn up by CLC/SC 9XA.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CENELEC 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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

Contents

Page

European foreword

This document [prEN 50159:2025] has been preprared by CLC/SC 9XA “Communication, signalling and processing systems”.

This document is currently submitted to the Enquiry.

The following dates are proposed:

• latest date by which the existence of this document has to be announced at national level	(doa)	dav + 6 months
• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	dav + 12 months
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	dav + 36 months (to be confirmed or modified when voting)

This document will supersede EN 50159:2010. and all of its amendments and corrigenda (if any).

prEN 50159:2025 includes the following significant technical changes with respect to EN 50159:2010:

Introduction

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

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.

The 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: transmission systems are closed,

– Category 2 and Category 3: transmission systems are open.

Application messages using Category 3 transmission systems need protection against unauthorised access. The specific cybersecurity requirements for Category 3 transmission systems are out of the scope of this document. For such systems, 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 tolerable, 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 IT security 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 50129:2018,[1] *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

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

IEC 63452,[2] *Rail applications - Cybersecurity*

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] As impacted by EN 5019:2018/AC:2019-04.

[2] Under preparation.

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: IEV 821-11-01]

3.1.2
access control
protection of system resources against unauthorized access

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

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

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

[SOURCE: IEV 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, modified — Note 2 to entry added]

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

[SOURCE: IEV 821-11-04]

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

[SOURCE: IEV 821-11-05]

3.1.7
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 negligible

[SOURCE: IEV 821-11-06]

3.1.8
communication
information transfer according to agreed conventions

[SOURCE: IEV 701-01-04]

3.1.9
confidentiality
<in cybersecurity>
assurance that information is not disclosed to unauthorized individuals, processes, or devices

[SOURCE: CLC/TS 50701:2023]

3.1.10
corrupted message
type of message error in which a data corruption occurs

[SOURCE: IEV 821-11-08]

3.1.11
countermeasure
<in 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]

3.1.12
cryptographic algorithm
algorithm based on the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms

[SOURCE: IEC 62443-1-1]

3.1.13
cybersecurity
<in railway application>
set of activities and measures taken with the objective to identify, protect, detect, respond, and recover to unauthorised 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 countermeasures, are not included in this document.

[SOURCE: CLC/TS 50701:2023]

3.1.14
cyclic redundancy check
<for communication in transmission systems>
cyclic code, used to protect messages from the influence of data corruption

[SOURCE: IEV 821-11-10]

3.1.15
data
<for communication in transmission systems>
part of a message which represents some information (see also user data, additional data, redundant data)

[SOURCE: IEV 821-11-11]

3.1.16
data corruption
alteration of data

[SOURCE: IEV 821-11-13]

3.1.17
defence
measure incorporated in the design of a safety-related communication system to counter particular hazards

[SOURCE: IEV 821-11-14]

3.1.18
delayed message
type of message error in which a message is received at a time later than intended

[SOURCE: IEV 821-11-15]

3.1.19
deleted message
type of message error in which a message is removed from the message stream

[SOURCE: IEV 821-11-16]

3.1.20
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

[SOURCE: IEV 821-11-17]

3.1.21
encryption
<of 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 added]

3.1.22
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: EN 50129:2018]

3.1.23
failure
loss of ability to perform as required

Note 1 to entry: Qualifiers, such as catastrophic, critical, major, minor, marginal and insignificant, may 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, may 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: EN 50129:2018]

3.1.24
fault
abnormal condition that could lead to an error in a system

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

[SOURCE: EN 50129:2018]

3.1.25
feedback message
response from a receiver to the sender, via a return channel

[SOURCE: IEV 821-11-21]

3.1.26
hazard
condition that can lead to an accident

[SOURCE: EN 50129:2018]

3.1.27
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

[SOURCE: EN 50129:2018]

3.1.28
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: IEV 903-01-04]

3.1.29
implicit data
additional data that is not transmitted but is known to the sender and receiver

[SOURCE: IEV 821-11-12]

3.1.30
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: IEV 171-01-01]

3.1.31
inserted message
type of message error in which an additional message is implanted in the message stream

[SOURCE: IEV 821-11-25]

3.1.32
integrity
<of information>
state in which information is complete and not altered

[SOURCE: IEV 821-11-26]

3.1.33
manipulation detection code
function of the whole message without secret key

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

[SOURCE: IEV 821-11-27]

3.1.34
masqueraded message
type of inserted message in which a non-authentic message is intentionally designed to appear to be authentic

[SOURCE: IEV 821-11-28]

3.1.35
message
<in transmission systems>
information which is transmitted in one or several packets from a sender to one or more receivers

[SOURCE: IEV 821-11-29]

3.1.36
message authentication code
cryptographic function of the whole message and a secret or public key

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

[SOURCE: IEV 821-11-30]

3.1.37
message encryption
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

Note 1 to entry: Message encryption does not provide protection against data corruption.

Note 2 to entry: The original definition was for “message enciphering”. However, in this document, encryption is more common.

[SOURCE: IEV 821-11-31, modified — Note 2 to entry added]

3.1.38
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: IEV 821-11-32]

3.1.39
message integrity
message in which information is complete and not altered

[SOURCE: IEV 821-11-33]

3.1.40
message stream
ordered set of messages

[SOURCE: IEV 821-11-34]

3.1.41
negligible risk
risk which is so low that it is not reasonable to implement additional measures

Note 1 to entry: For negligible risks, no further requirements need to be specified. Negligible risks are considered as insignificant and adequately controlled.

3.1.42
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

[SOURCE: IEV 821-11-36]

3.1.43
random failure
failure that occurs randomly in time

[SOURCE: IEV 821-11-38]

3.1.44
redundancy check
type of check that a predefined relationship exists between redundant data and user data within a message, to prove message integrity

[SOURCE: IEV 821-11-39]

3.1.45
redundant data
additional data, derived, by a safety-related transmission function, from the user data

[SOURCE: IEV 821-11-40]

3.1.46
relative time stamp
time stamp referenced to the local clock of an entity. In general there is no relationship to clocks of other entities

[SOURCE: IEV 821-11-41]

3.1.47
repeated message
type of message error in which a single message is received more than once

[SOURCE: IEV 821-11-42]

3.1.48
re-sequenced message
type of message error in which the order of messages in the message stream is changed

[SOURCE: IEV 821-11-43]

3.1.49
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: IEV 821-11-44]

3.1.50
safety
freedom from unacceptable levels of risk

[SOURCE: EN 50129:2018]

3.1.51
safety case
documented demonstration that the product complies with the specified safety requirements

[SOURCE: EN 50129:2018]

3.1.52
safety code
redundant data included in a safety-related message to permit data corruptions to be detected by the safety-related transmission function

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

[SOURCE: IEV 821-11-45] adapted

3.1.53
safety integrity level
one of a number of defined discrete levels for specifying the safety integrity requirements of safety-related functions to be allocated to the safety-related systems

[SOURCE: EN 50129:2018]